



CLI Reference

FortiProxy 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



July 10, 2025

FortiProxy 7.6.3 CLI Reference

45-763-1081269-20250710

TABLE OF CONTENTS

Change log	72
FortiProxy CLI Interface	73
CLI configuration commands	74
alertemail	75
config alertemail setting	75
antivirus	82
config antivirus exempt-list	82
config antivirus profile	83
config antivirus quarantine	113
config antivirus settings	117
application	120
config application custom	120
config application group	121
config application list	122
config application name	131
config application rule-settings	133
authentication	134
config authentication rule	134
config authentication scheme	137
config authentication setting	140
automation	144
config automation setting	144
casb	145
config casb profile	145
config casb saas-application	148
config casb user-activity	149
certificate	156
config certificate ca	156
config certificate crt	158
config certificate hsm-local	159
config certificate local	164
config certificate remote	169
dlp	171
config dlp data-type	171
config dlp dictionary	173
config dlp exact-data-match	175
config dlp filepattern	176
config dlp fp-doc-source	179
config dlp profile	183
config dlp sensitivity	187
config dlp sensor	188
config dlp settings	189
dnsfilter	191
config dnsfilter domain-filter	191
config dnsfilter profile	192

emailfilter	199
config emailfilter block-allow-list	199
config emailfilter bword	201
config emailfilter dnsbl	203
config emailfilter fortishield	205
config emailfilter iptrust	205
config emailfilter mheader	207
config emailfilter options	208
config emailfilter profile	209
endpoint-control	217
config endpoint-control fctems	217
config endpoint-control fctems-override	222
config endpoint-control settings	227
file-filter	228
config file-filter profile	228
firewall	231
config firewall access-proxy	232
config firewall access-proxy6	269
config firewall access-proxy-ssh-client-cert	306
config firewall access-proxy-virtual-host	308
config firewall address	309
config firewall address6	315
config firewall addrgrp	319
config firewall addrgrp6	322
config firewall auth-portal	323
config firewall central-snat-map	324
config firewall city	326
config firewall country	326
config firewall decrypted-traffic-mirror	327
config firewall global	328
config firewall identity-based-route	329
config firewall internet-service	330
config firewall internet-service-addition	332
config firewall internet-service-append	333
config firewall internet-service-botnet	334
config firewall internet-service-custom	335
config firewall internet-service-custom-group	337
config firewall internet-service-definition	337
config firewall internet-service-extension	339
config firewall internet-service-group	343
config firewall internet-service-ipbl-reason	344
config firewall internet-service-ipbl-vendor	344
config firewall internet-service-list	345
config firewall internet-service-name	345
config firewall internet-service-owner	346
config firewall internet-service-reputation	347
config firewall internet-service-sld	348
config firewall internet-service-subapp	348
config firewall ippool	349

config firewall ippool6	349
config firewall network-service-dynamic	350
config firewall on-demand-sniffer	351
config firewall policy	353
config firewall profile-group	366
config firewall profile-protocol-options	368
config firewall proxy-address	393
config firewall proxy-address6	398
config firewall proxy-addrgrp	402
config firewall proxy-addrgrp6	404
config firewall region	405
config firewall response-shaping-policy	406
config firewall schedule group	408
config firewall schedule onetime	409
config firewall schedule recurring	410
config firewall service category	411
config firewall service custom	412
config firewall service group	416
config firewall shaper per-ip-shaper	417
config firewall shaper traffic-shaper	418
config firewall shaping-policy	421
config firewall shaping-profile	425
config firewall sniffer	426
config firewall ssh host-key	428
config firewall ssh local-ca	430
config firewall ssh local-key	430
config firewall ssh setting	431
config firewall ssl default-certificate	432
config firewall ssl keyring-list	433
config firewall ssl setting	433
config firewall ssl-server	435
config firewall ssl-ssh-profile	438
config firewall traffic-class	471
config firewall ttl-policy	471
config firewall vendor-mac	472
config firewall vendor-mac-summary	473
config firewall vip	473
config firewall vipgrp	509
config firewall wildcard-fqdn custom	510
config firewall wildcard-fqdn group	511
ftp-proxy	513
config ftp-proxy explicit	513
hardware	516
config hardware cpu	516
config hardware memory	516
config hardware nic	516
config hardware status	517
icap	518
config icap local-server	518

config icap profile	521
config icap remote-server	530
config icap remote-server-group	531
image-analyzer	533
config image-analyzer profile	533
ips	538
config ips custom	538
config ips decoder	540
config ips global	540
config ips rule	544
config ips rule-settings	546
config ips sensor	546
config ips session	552
config ips settings	553
config ips view-map	554
ipsec	555
config ipsec tunnel	555
isolator	556
config isolator profile	556
config isolator setting	557
l2vpn	559
config l2vpn evpn instance	559
config l2vpn evpn table	559
log	560
config log custom-field	561
config log disk filter	562
config log disk setting	565
config log eventfilter	571
config log fortianalyzer filter	575
config log fortianalyzer override-filter	579
config log fortianalyzer override-setting	582
config log fortianalyzer setting	587
config log fortianalyzer2 filter	591
config log fortianalyzer2 override-filter	595
config log fortianalyzer2 override-setting	599
config log fortianalyzer2 setting	603
config log fortianalyzer3 filter	608
config log fortianalyzer3 override-filter	611
config log fortianalyzer3 override-setting	615
config log fortianalyzer3 setting	620
config log fortianalyzer-cloud filter	624
config log fortianalyzer-cloud override-filter	628
config log fortianalyzer-cloud override-setting	631
config log fortianalyzer-cloud setting	632
config log fortiguard filter	636
config log fortiguard override-filter	639
config log fortiguard override-setting	643
config log fortiguard setting	644

config log gui-display	647
config log memory filter	648
config log memory global-setting	652
config log memory setting	652
config log null-device filter	653
config log null-device setting	656
config log setting	657
config log syslogd filter	661
config log syslogd override-filter	665
config log syslogd override-setting	669
config log syslogd setting	674
config log syslogd2 filter	679
config log syslogd2 override-filter	682
config log syslogd2 override-setting	686
config log syslogd2 setting	691
config log syslogd3 filter	696
config log syslogd3 override-filter	700
config log syslogd3 override-setting	703
config log syslogd3 setting	708
config log syslogd4 filter	714
config log syslogd4 override-filter	717
config log syslogd4 override-setting	721
config log syslogd4 setting	726
config log tacacs+accounting filter	731
config log tacacs+accounting setting	732
config log tacacs+accounting2 filter	733
config log tacacs+accounting2 setting	734
config log tacacs+accounting3 filter	735
config log tacacs+accounting3 setting	736
config log threat-weight	737
config log webtrends filter	749
config log webtrends setting	752
mgmt-data	754
config mgmt-data status	754
oaas	755
config oaas status	755
report	756
config report layout	756
config report setting	764
config report sql status	765
router	766
config router policy	766
config router static	768
config router static6	770
rule	773
config rule fwp	773
config rule otdt	775
config rule otvp	777

ssh-filter	780
config ssh-filter profile	780
system	783
config system accprofile	786
config system acme	798
config system admin	799
config system affinity-interrupt	807
config system affinity-packet-redistribution	808
config system alarm	808
config system alias	812
config system api-user	812
config system arp	814
config system arp-table	814
config system automation-action	815
config system automation-condition	820
config system automation-destination	822
config system automation-stitch	822
config system automation-trigger	824
config system autoupdate schedule	829
config system autoupdate tunneling	830
config system auto-install	831
config system auto-script	832
config system auto-update status	833
config system auto-update versions	833
config system central-management	833
config system central-mgmt	838
config system checksum status	839
config system cloud-service	839
config system cmdb	840
config system console	840
config system csf	841
config system custom-language	847
config system ddns	848
config system device-upgrade	851
config system dhcp server	854
config system dhcp6 server	866
config system dns	869
config system dns-database	873
config system dns-server	876
config system dscp-based-priority	877
config system email-server	878
config system external-resource	880
config system fabric-vpn	883
config system federated-upgrade	887
config system fips-cc	891
config system fortianalyzer-connectivity	892
config system fortiguard	892
config system fortiguard-log-service	903
config system fortiguard-service	903

config system fortindr	903
config system fortisandbox	904
config system fsso-polling	906
config system ftm-push	907
config system geoip-country	908
config system geoip-override	908
config system global	910
config system gre-tunnel	956
config system ha	958
config system ha-lic	970
config system ha-monitor	970
config system ha-nonsync-csum	971
config system info admin ssh	971
config system info admin status	972
config system interface	972
config system ipam	1008
config system ips	1012
config system ips-urlfilter-dns	1013
config system ips-urlfilter-dns6	1013
config system ipv6-neighbor-cache	1014
config system ip-conflict status	1015
config system link-monitor	1015
config system management-tunnel	1020
config system mgmt-csum	1022
config system nethsm	1022
config system network-visibility	1026
config system ntp	1027
config system object-tagging	1030
config system password-policy	1032
config system password-policy-guest-admin	1034
config system performance status	1036
config system performance top	1037
config system probe-response	1037
config system proxy-arp	1039
config system ptp	1039
config system replacemsg admin	1041
config system replacemsg alertmail	1042
config system replacemsg auth	1043
config system replacemsg automation	1044
config system replacemsg custom-message	1045
config system replacemsg fortiguard-wf	1046
config system replacemsg ftp	1047
config system replacemsg http	1048
config system replacemsg icap	1049
config system replacemsg mail	1050
config system replacemsg nac-quar	1051
config system replacemsg spam	1052
config system replacemsg sslvpn	1053
config system replacemsg traffic-quota	1054

config system replacemsg utm	1055
config system replacemsg webproxy	1056
config system replacemsg-group	1057
config system replacemsg-image	1070
config system resource-limits	1071
config system saml	1073
config system sdn-connector	1077
config system sdn-proxy	1086
config system session	1087
config system session6	1087
config system session-ttl	1087
config system settings	1088
config system sms-server	1104
config system snmp community	1104
config system snmp mib-view	1112
config system snmp sysinfo	1112
config system snmp user	1114
config system source-ip status	1120
config system span-port	1120
config system speed-test-schedule	1121
config system speed-test-server	1124
config system speed-test-setting	1125
config system ssh-config	1126
config system sso-admin	1130
config system sso-forticloud-admin	1131
config system sso-fortigate-cloud-admin	1131
config system startup-error-log	1132
config system status	1132
config system storage	1132
config system timezone	1134
config system vdom	1134
config system vdom-dns	1135
config system vdom-exception	1137
config system vdom-link	1140
config system vdom-property	1140
config system vdom-radius-server	1142
config system vne-tunnel	1142
config system vxlan	1144
config system wccp	1145
config system zone	1149
test	1151
config test acd	1153
config test acsd	1153
config test autod	1153
config test awsd	1154
config test azd	1154
config test bfd	1154
config test cloudapid	1155
config test cmdbsvr	1155

config test csfd	1156
config test ddnsd	1156
config test dhcp6c	1156
config test dhcp6r	1157
config test dhcprelay	1157
config test dlpfingerprint	1157
config test dlpfpcache	1158
config test dnsproxy	1158
config test dsd	1159
config test eap_supp	1159
config test evpn	1159
config test fas	1160
config test fcnacd	1160
config test fds_notify	1160
config test fgtlogd	1161
config test fnbamd	1161
config test forticldd	1162
config test forticron	1162
config test fsd	1162
config test fsvrd	1163
config test gcpd	1163
config test harelay	1163
config test hasync	1164
config test hatalk	1164
config test ibmd	1165
config test imap	1165
config test init	1165
config test iotd	1166
config test ipamd	1166
config test ipamsd	1166
config test ipldbd	1167
config test ipsengine	1167
config test ipsmonitor	1168
config test ipsufd	1168
config test kmipd	1168
config test kubed	1169
config test l2tpcd	1169
config test lnkmt	1169
config test locallogd	1170
config test miglogd	1170
config test mrd	1171
config test netxd	1171
config test nntp	1171
config test ocid	1172
config test openstackd	1172
config test ovrd	1172
config test pcpc	1173
config test pop3	1173
config test pptpcd	1174

config test quarantined	1174
config test radiusd	1174
config test radius-das	1175
config test radvd	1175
config test reportd	1175
config test sdncd	1176
config test sdnd	1176
config test sepmc	1177
config test sessionsync	1177
config test sfupgraded	1177
config test smtp	1178
config test snmpd	1178
config test syslogd	1178
config test updated	1179
config test uploadd	1179
config test urlfilter	1180
config test vned	1180
config test wad	1180
config test wccpd	1181
config test wf_monitor	1181
config test wiredapd	1181
user	1183
config user adgrp	1183
config user certificate	1184
config user domain-controller	1185
config user exchange	1189
config user external-identity-provider	1192
config user fortitoken	1194
config user fsso	1195
config user fsso-polling	1199
config user group	1201
config user krb-keytab	1206
config user ldap	1207
config user local	1216
config user oidc	1220
config user password-policy	1223
config user peer	1225
config user peergrp	1227
config user pop3	1227
config user radius	1229
config user saml	1244
config user security-exempt-list	1248
config user setting	1249
config user tacacs+	1254
videofilter	1257
config videofilter keyword	1257
config videofilter profile	1258
config videofilter youtube-key	1261
virtual-patch	1262

config virtual-patch profile	1262
vpn	1264
config vpn certificate ca	1264
config vpn certificate crt	1266
config vpn certificate hsm-local	1268
config vpn certificate local	1272
config vpn certificate ocsf-server	1277
config vpn certificate remote	1278
config vpn certificate setting	1279
config vpn ipsec phase1-interface	1285
config vpn ipsec phase2-interface	1304
config vpn qkd	1312
waf	1314
config waf main-class	1314
config waf profile	1314
config waf signature	1339
config waf sub-class	1340
wanopt	1341
config wanopt auth-group	1341
config wanopt cache-service	1342
config wanopt content-delivery-network-rule	1344
config wanopt peer	1350
config wanopt profile	1350
config wanopt remote-storage	1359
config wanopt settings	1360
web-proxy	1361
config web-proxy debug-url	1361
config web-proxy dynamic-bypass	1362
config web-proxy explicit-proxy	1363
config web-proxy fast-fallback	1370
config web-proxy forward-server	1371
config web-proxy forward-server-group	1373
config web-proxy global	1375
config web-proxy implicit-proxy-rule	1381
config web-proxy implicit-proxy-setting	1382
config web-proxy isolator-server	1383
config web-proxy pac-policy	1384
config web-proxy profile	1385
config web-proxy redirect-profile	1390
config web-proxy url-list	1392
config web-proxy url-match	1393
config web-proxy wisp	1394
webcache	1396
config webcache prefetch	1396
config webcache reverse-cache-server	1397
config webcache settings	1398
config webcache user-agent	1402
webfilter	1403

config webfilter categories	1403
config webfilter content	1403
config webfilter content-header	1405
config webfilter domain-list	1406
config webfilter fortiguard	1407
config webfilter ftgd-local-cat	1410
config webfilter ftgd-local-rating	1410
config webfilter ftgd-local-risk	1411
config webfilter ftgd-risk-level	1412
config webfilter ftgd-statistics	1413
config webfilter ips-urlfilter-cache-setting	1413
config webfilter ips-urlfilter-setting	1413
config webfilter ips-urlfilter-setting6	1414
config webfilter override	1415
config webfilter override-usr	1416
config webfilter profile	1417
config webfilter search-engine	1435
config webfilter status	1436
config webfilter urlfilter	1436
config webfilter url-list	1440
ztna	1442
config ztna connector-service-edge	1442
config ztna reverse-connector	1443
config ztna service-connector	1444
config ztna traffic-forward-proxy	1447
config ztna web-portal	1448
config ztna web-portal-bookmark	1453
config ztna web-proxy	1459
CLI diagnose commands	1493
diagnose alertconsole	1494
diagnose alertconsole clear	1495
diagnose alertconsole fgd-retrieve	1495
diagnose alertconsole list	1495
diagnose alertconsole test	1495
diagnose antivirus	1495
diagnose antivirus database-info	1496
diagnose antivirus outbreak-prevention	1496
diagnose antivirus outbreak-prevention statistics	1496
diagnose antivirus outbreak-prevention statistics flush	1496
diagnose antivirus outbreak-prevention statistics list	1496
diagnose antivirus quarantine	1496
diagnose antivirus quarantine delete	1497
diagnose antivirus quarantine list	1497
diagnose antivirus quarantine purge	1497
diagnose antivirus test	1497
diagnose automation	1498
diagnose automation test	1498
diagnose autoupdate	1498

diagnose autoupdate downgrade	1498
diagnose autoupdate downgrade disable	1498
diagnose autoupdate downgrade enable	1499
diagnose autoupdate status	1499
diagnose autoupdate versions	1499
diagnose casb	1499
diagnose casb build	1500
diagnose casb show	1500
diagnose casb show app-details	1500
diagnose casb show app-domains	1500
diagnose casb show applications	1500
diagnose casb show apps	1500
diagnose casb show domains	1501
diagnose casb show isdb	1501
diagnose casb show isdb-all	1501
diagnose casb show isdb-name	1501
diagnose casb show isdb-uuid	1501
diagnose casb verify	1501
diagnose casb verify casb-isdb	1502
diagnose debug	1502
diagnose debug admin	1509
diagnose debug admin error-log	1509
diagnose debug application	1509
diagnose debug application acd	1510
diagnose debug application acid	1510
diagnose debug application alarmd	1510
diagnose debug application alertmail	1510
diagnose debug application alicloud-ha	1510
diagnose debug application alicloud-sdn	1511
diagnose debug application authd	1511
diagnose debug application autod	1511
diagnose debug application awsd	1511
diagnose debug application azd	1512
diagnose debug application azd-ha	1512
diagnose debug application bfdd	1512
diagnose debug application cert-update	1512
diagnose debug application chassis	1513
diagnose debug application clearpass	1513
diagnose debug application cloudapid	1513
diagnose debug application cloudinitd	1513
diagnose debug application cmp	1513
diagnose debug application crt-update	1514
diagnose debug application crwl	1514
diagnose debug application csfd	1514
diagnose debug application ddnsd	1514
diagnose debug application dhcp6c	1515
diagnose debug application dhcp6r	1515
diagnose debug application dhcp6s	1515
diagnose debug application dhcpc	1515

diagnose debug application dhcprelay	1516
diagnose debug application dhcps	1516
diagnose debug application dlpfingerprint	1516
diagnose debug application dnp	1516
diagnose debug application dnsproxy	1517
diagnose debug application eap_proxy	1517
diagnose debug application eap_supp	1517
diagnose debug application est	1517
diagnose debug application evpnd	1517
diagnose debug application extenderd	1518
diagnose debug application fclld	1518
diagnose debug application fcnacd	1518
diagnose debug application fds_notify	1518
diagnose debug application fgd_alert	1519
diagnose debug application fgfmd	1519
diagnose debug application fgtlogd	1519
diagnose debug application fnbamd	1519
diagnose debug application foauthd	1520
diagnose debug application forticldd	1520
diagnose debug application forticron	1520
diagnose debug application fsd	1520
diagnose debug application fsso_ldap	1520
diagnose debug application fssod	1521
diagnose debug application fsvrd	1521
diagnose debug application ftm-push	1521
diagnose debug application garpd	1521
diagnose debug application gcpd	1522
diagnose debug application hamonitord	1522
diagnose debug application harelay	1522
diagnose debug application hasync	1522
diagnose debug application hatalk	1523
diagnose debug application httpsd	1523
diagnose debug application ibmd	1523
diagnose debug application icond	1523
diagnose debug application imap	1524
diagnose debug application init	1524
diagnose debug application iotd	1524
diagnose debug application ipamd	1524
diagnose debug application ipamsd	1524
diagnose debug application ipldbd	1525
diagnose debug application ipsengine	1525
diagnose debug application ipsmonitor	1525
diagnose debug application ipsufd	1525
diagnose debug application iptables	1526
diagnose debug application kmiglogd	1526
diagnose debug application kmipd	1526
diagnose debug application kubed	1526
diagnose debug application l2tp	1527
diagnose debug application link-monitor	1527

diagnose debug application link-monitor-passive	1527
diagnose debug application lldptx	1527
diagnose debug application locallogd	1527
diagnose debug application lpmc	1528
diagnose debug application miglogd	1528
diagnose debug application mrd	1528
diagnose debug application nethsm	1528
diagnose debug application netxd	1529
diagnose debug application nntp	1529
diagnose debug application nodejs	1529
diagnose debug application npd	1529
diagnose debug application ntnxd	1530
diagnose debug application ntpd	1530
diagnose debug application oaas_agent	1530
diagnose debug application ocid	1530
diagnose debug application openstackd	1531
diagnose debug application ovrd	1531
diagnose debug application pcpc	1531
diagnose debug application pop3	1531
diagnose debug application ppp	1531
diagnose debug application pppoed	1532
diagnose debug application pptp	1532
diagnose debug application pptpc	1532
diagnose debug application proxy	1532
diagnose debug application ptpd	1533
diagnose debug application quarantine	1533
diagnose debug application radius-das	1533
diagnose debug application radiusd	1533
diagnose debug application radvd	1534
diagnose debug application reportd	1534
diagnose debug application route-tag	1534
diagnose debug application rt-router	1534
diagnose debug application samld	1534
diagnose debug application sapd	1535
diagnose debug application sccp	1535
diagnose debug application scep	1535
diagnose debug application sdncd	1535
diagnose debug application sdwan	1536
diagnose debug application sepmd	1536
diagnose debug application server-probe	1536
diagnose debug application sessionsync	1536
diagnose debug application sflowd	1537
diagnose debug application sfupgraded	1537
diagnose debug application sip	1537
diagnose debug application smbcd	1537
diagnose debug application smtp	1537
diagnose debug application snmpd	1538
diagnose debug application spareblock	1538
diagnose debug application speedtest	1538

diagnose debug application speedtestd	1538
diagnose debug application sshd	1539
diagnose debug application syslogd	1539
diagnose debug application tvc	1539
diagnose debug application update	1539
diagnose debug application uploadd	1540
diagnose debug application urlfilter	1540
diagnose debug application vmtoolsd	1540
diagnose debug application vmwd	1540
diagnose debug application vned	1540
diagnose debug application vpd	1541
diagnose debug application vrrpd	1541
diagnose debug application wabcs	1541
diagnose debug application waocs	1541
diagnose debug application wccpd	1542
diagnose debug application wf_monitor	1542
diagnose debug authd	1542
diagnose debug authd clear	1542
diagnose debug authd fsso	1542
diagnose debug authd fsso add-address	1543
diagnose debug authd fsso clear-logons	1543
diagnose debug authd fsso del-address	1543
diagnose debug authd fsso filter	1543
diagnose debug authd fsso filter clear	1543
diagnose debug authd fsso filter group	1544
diagnose debug authd fsso filter server	1544
diagnose debug authd fsso filter source	1544
diagnose debug authd fsso filter user	1544
diagnose debug authd fsso flush-address	1544
diagnose debug authd fsso flush-address-all	1545
diagnose debug authd fsso list	1545
diagnose debug authd fsso refresh-groups	1545
diagnose debug authd fsso refresh-logons	1545
diagnose debug authd fsso server-status	1545
diagnose debug authd fsso show-address	1545
diagnose debug authd fsso summary	1546
diagnose debug authd memory	1546
diagnose debug backtrace	1546
diagnose debug cli	1546
diagnose debug cloudinit	1546
diagnose debug cloudinit clear	1546
diagnose debug cloudinit show	1547
diagnose debug cmdb-trace	1547
diagnose debug cmdb-walk	1547
diagnose debug config-error-log	1547
diagnose debug config-error-log clear	1547
diagnose debug config-error-log read	1548
diagnose debug console	1548
diagnose debug console no-user-log-msg	1548

diagnose debug console no-user-log-msg disable	1548
diagnose debug console no-user-log-msg enable	1548
diagnose debug console retry-log-msg	1548
diagnose debug console retry-log-msg disable	1549
diagnose debug console retry-log-msg enable	1549
diagnose debug console send	1549
diagnose debug console timestamp	1549
diagnose debug console timestamp disable	1549
diagnose debug console timestamp enable	1550
diagnose debug crashlog	1550
diagnose debug crashlog clear	1550
diagnose debug crashlog get	1550
diagnose debug crashlog history	1550
diagnose debug crashlog interval	1550
diagnose debug disable	1551
diagnose debug duration	1551
diagnose debug enable	1551
diagnose debug flow	1551
diagnose debug flow filter	1551
diagnose debug flow filter addr	1552
diagnose debug flow filter clear	1552
diagnose debug flow filter daddr	1552
diagnose debug flow filter dport	1552
diagnose debug flow filter negate	1553
diagnose debug flow filter negate addr	1553
diagnose debug flow filter negate daddr	1553
diagnose debug flow filter negate dport	1554
diagnose debug flow filter negate port	1554
diagnose debug flow filter negate proto	1554
diagnose debug flow filter negate saddr	1554
diagnose debug flow filter negate sport	1555
diagnose debug flow filter negate vd	1555
diagnose debug flow filter port	1555
diagnose debug flow filter proto	1555
diagnose debug flow filter saddr	1556
diagnose debug flow filter sport	1556
diagnose debug flow filter vd	1556
diagnose debug flow filter vd-name	1557
diagnose debug flow filter6	1557
diagnose debug flow filter6 addr	1557
diagnose debug flow filter6 clear	1558
diagnose debug flow filter6 daddr	1558
diagnose debug flow filter6 dport	1558
diagnose debug flow filter6 negate	1559
diagnose debug flow filter6 negate addr	1559
diagnose debug flow filter6 negate daddr	1559
diagnose debug flow filter6 negate dport	1559
diagnose debug flow filter6 negate port	1560
diagnose debug flow filter6 negate proto	1560

diagnose debug flow filter6 negate saddr	1560
diagnose debug flow filter6 negate sport	1560
diagnose debug flow filter6 negate vd	1561
diagnose debug flow filter6 port	1561
diagnose debug flow filter6 proto	1561
diagnose debug flow filter6 saddr	1561
diagnose debug flow filter6 sport	1562
diagnose debug flow filter6 vd	1562
diagnose debug flow filter6 vd-name	1562
diagnose debug flow show	1563
diagnose debug flow show function-name	1563
diagnose debug flow show function-name disable	1563
diagnose debug flow show function-name enable	1563
diagnose debug flow trace	1563
diagnose debug flow trace start	1564
diagnose debug flow trace start6	1564
diagnose debug flow trace stop	1564
diagnose debug flow trace stop6	1564
diagnose debug fortism	1564
diagnose debug fortism enable	1565
diagnose debug fsso-polling	1565
diagnose debug fsso-polling client	1565
diagnose debug fsso-polling detail	1565
diagnose debug fsso-polling group	1565
diagnose debug fsso-polling refresh-user	1566
diagnose debug fsso-polling set-log-source	1566
diagnose debug fsso-polling summary	1566
diagnose debug fsso-polling user	1566
diagnose debug info	1566
diagnose debug kernel	1567
diagnose debug kernel ha	1567
diagnose debug kernel level	1567
diagnose debug kernel log	1567
diagnose debug kernel log clear	1567
diagnose debug kernel log show	1568
diagnose debug kernel sysrq	1568
diagnose debug kernel sysrq command	1568
diagnose debug kernel sysrq command crash	1568
diagnose debug kernel sysrq disable	1568
diagnose debug kernel sysrq enable	1568
diagnose debug kernel sysrq status	1569
diagnose debug rating	1569
diagnose debug remote-extender	1569
diagnose debug remote-extender extenderd	1569
diagnose debug remote-extender modem-manager	1569
diagnose debug report	1570
diagnose debug report reset	1570
diagnose debug reset	1570
diagnose debug sdnc	1570

diagnose debug sdnc valgrind	1570
diagnose debug sdnc valgrind disable	1570
diagnose debug sdnc valgrind enable	1571
diagnose debug sdnc valgrind log	1571
diagnose debug sdnc valgrind log clear	1571
diagnose debug sdnc valgrind log show	1571
diagnose debug sdnc valgrind memcheck	1571
diagnose debug sdnc valgrind memcheck_less	1571
diagnose debug sdnc valgrind status	1572
diagnose debug sql-log-error	1572
diagnose debug sql-log-error clear	1572
diagnose debug sql-log-error read	1572
diagnose debug sql-log-error status	1572
diagnose debug traffic	1572
diagnose debug traffic dump-debug	1573
diagnose debug traffic history	1573
diagnose debug traffic interface	1573
diagnose debug traffic peek	1573
diagnose debug urlfilter	1573
diagnose debug urlfilter src-addr	1574
diagnose debug urlfilter test-url	1574
diagnose debug urlfilter valgrind	1574
diagnose debug urlfilter valgrind disable	1574
diagnose debug urlfilter valgrind enable	1574
diagnose debug urlfilter valgrind log	1575
diagnose debug urlfilter valgrind log clear	1575
diagnose debug urlfilter valgrind log show	1575
diagnose debug urlfilter valgrind memcheck	1575
diagnose debug urlfilter valgrind memcheck_less	1575
diagnose debug urlfilter valgrind status	1575
diagnose debug user	1576
diagnose debug user hash	1576
diagnose debug user list	1576
diagnose debug vm-print-license	1576
diagnose disktest	1576
diagnose disktest block	1577
diagnose disktest block 1	1577
diagnose disktest block 16	1577
diagnose disktest block 256	1577
diagnose disktest block 4	1577
diagnose disktest block 64	1577
diagnose disktest device	1578
diagnose disktest run	1578
diagnose disktest size	1578
diagnose disktest time	1578
diagnose emailfilter	1579
diagnose emailfilter bword	1579
diagnose emailfilter bword matchfilter	1579
diagnose emailfilter fortishield	1579

diagnose emailfilter fortishield servers	1579
diagnose emailfilter fortishield statistics	1580
diagnose emailfilter fortishield statistics flush	1580
diagnose emailfilter fortishield statistics list	1580
diagnose endpoint	1580
diagnose endpoint avatar	1582
diagnose endpoint avatar allow-nodisk	1583
diagnose endpoint avatar cleanup	1583
diagnose endpoint avatar find	1583
diagnose endpoint avatar find fingerprint	1583
diagnose endpoint avatar find uid	1583
diagnose endpoint avatar list	1584
diagnose endpoint avatar list active	1584
diagnose endpoint avatar list all	1584
diagnose endpoint avatar list inactive	1584
diagnose endpoint avatar purge-all	1585
diagnose endpoint debug-zone	1585
diagnose endpoint debug-zone background-debug	1585
diagnose endpoint debug-zone dump	1585
diagnose endpoint debug-zone set-lls-quota	1585
diagnose endpoint ec-shm	1586
diagnose endpoint ec-shm delete	1586
diagnose endpoint ec-shm find-by-ipvd	1586
diagnose endpoint ec-shm find-by-uid	1586
diagnose endpoint ec-shm list	1587
diagnose endpoint ec-shm summary	1587
diagnose endpoint ec-shm update-by-json	1587
diagnose endpoint fctems	1587
diagnose endpoint fctems api-status	1588
diagnose endpoint fctems api-status clear	1588
diagnose endpoint fctems cloud-server	1588
diagnose endpoint fctems custom	1588
diagnose endpoint fctems ec-shm-dump	1589
diagnose endpoint fctems get-pub-addr	1589
diagnose endpoint fctems info	1589
diagnose endpoint fctems info pause	1589
diagnose endpoint fctems info pre-master-key	1589
diagnose endpoint fctems info protocol	1590
diagnose endpoint fctems info repeat	1590
diagnose endpoint fctems info repeat data-in	1590
diagnose endpoint fctems info repeat data-out	1590
diagnose endpoint fctems info repeat header-in	1590
diagnose endpoint fctems info repeat header-out	1591
diagnose endpoint fctems info repeat ssl-data-in	1591
diagnose endpoint fctems info repeat ssl-data-out	1591
diagnose endpoint fctems info repeat textinfo	1591
diagnose endpoint fctems info reset	1592
diagnose endpoint fctems info resume	1592
diagnose endpoint fctems json	1592

diagnose endpoint fctems json deep-inspect-cert-sync	1592
diagnose endpoint fctems json gateway-mac-request	1592
diagnose endpoint fctems queue-complete-calls	1592
diagnose endpoint fctems test-authorization	1593
diagnose endpoint fctems test-connectivity	1593
diagnose endpoint fctems wss-cert-skip-check	1593
diagnose endpoint filter	1593
diagnose endpoint filter avatar-fingerprint	1593
diagnose endpoint filter clear	1594
diagnose endpoint filter ems-sn	1594
diagnose endpoint filter ftcl-uid	1594
diagnose endpoint filter list	1594
diagnose endpoint filter record-debug-log	1594
diagnose endpoint filter show-large-data	1595
diagnose endpoint lls-comm	1595
diagnose endpoint lls-comm connect	1595
diagnose endpoint lls-comm disconnect	1595
diagnose endpoint lls-comm recv	1595
diagnose endpoint lls-comm send	1596
diagnose endpoint lls-comm send echo	1596
diagnose endpoint lls-comm send general	1596
diagnose endpoint lls-comm send general get-index	1596
diagnose endpoint lls-comm send general register	1596
diagnose endpoint lls-comm send general unregister	1596
diagnose endpoint lls-comm send ping	1597
diagnose endpoint lls-comm send ping set-interval	1597
diagnose endpoint lls-comm send ztna	1597
diagnose endpoint lls-comm send ztna find-ip-vdom	1597
diagnose endpoint lls-comm send ztna find-uid	1597
diagnose endpoint lls-comm send ztna message-format	1598
diagnose endpoint lls-comm send ztna subscribe-all	1598
diagnose endpoint lls-comm send ztna unsubscribe-all	1598
diagnose endpoint lls-comm send ztna unsubscribe-uid	1598
diagnose endpoint lls-comm status	1599
diagnose endpoint tags	1599
diagnose endpoint tags remove-by-id	1599
diagnose endpoint tags remove-by-name	1599
diagnose endpoint tags remove-by-name-legacy	1600
diagnose endpoint tags remove-by-sn	1600
diagnose endpoint tags test-common-tag-update	1600
diagnose fdsm	1600
diagnose fdsm account-info	1601
diagnose fdsm central-mgmt-status	1601
diagnose fdsm cfg-diff	1601
diagnose fdsm cfg-download	1602
diagnose fdsm cfg-list	1602
diagnose fdsm cfg-upload	1602
diagnose fdsm contract-controller-update	1602
diagnose fdsm fap-fsw-contract-download	1603

diagnose fdsm fc-installer-download	1603
diagnose fdsm fds-update	1603
diagnose fdsm fmg-auto-discovery-status	1603
diagnose fdsm forticlient-net-info	1603
diagnose fdsm forticlient-update	1604
diagnose fdsm fortix-download	1604
diagnose fdsm fortix-latest-ver	1604
diagnose fdsm fortisw-download	1604
diagnose fdsm fortisw-latest-ver	1604
diagnose fdsm ftk-activate	1605
diagnose fdsm image-download	1605
diagnose fdsm image-list	1605
diagnose fdsm image-upgrade-matrix	1605
diagnose fdsm log-controller-update	1605
diagnose fdsm message-update	1606
diagnose fdsm modem-list	1606
diagnose fdsm report-download	1606
diagnose fdsm report-list	1606
diagnose firewall	1606
diagnose firewall auth	1608
diagnose firewall auth clear	1609
diagnose firewall auth filter	1609
diagnose firewall auth filter clear	1609
diagnose firewall auth filter group	1609
diagnose firewall auth filter mac	1609
diagnose firewall auth filter method	1610
diagnose firewall auth filter policy	1610
diagnose firewall auth filter source	1610
diagnose firewall auth filter source6	1610
diagnose firewall auth filter user	1611
diagnose firewall auth ipv6	1611
diagnose firewall auth ipv6 clear	1611
diagnose firewall auth ipv6 list	1611
diagnose firewall auth list	1611
diagnose firewall auth mac	1611
diagnose firewall auth mac clear	1612
diagnose firewall auth mac list	1612
diagnose firewall dynamic	1612
diagnose firewall dynamic address	1612
diagnose firewall dynamic list	1612
diagnose firewall dynamic test-common-tag-update	1613
diagnose firewall dynamic6	1613
diagnose firewall dynamic6 address	1613
diagnose firewall dynamic6 list	1613
diagnose firewall fqdn	1613
diagnose firewall fqdn get-ip	1614
diagnose firewall fqdn get-mac	1614
diagnose firewall fqdn getinfo-ip	1614
diagnose firewall fqdn getinfo-mac	1614

diagnose firewall fqdn list-all	1614
diagnose firewall fqdn list-ip	1615
diagnose firewall fqdn list-mac	1615
diagnose firewall fqdn6	1615
diagnose firewall fqdn6 get	1615
diagnose firewall fqdn6 list	1615
diagnose firewall internet-service	1615
diagnose firewall internet-service list	1616
diagnose firewall internet-service-app-ctrl	1616
diagnose firewall internet-service-cache	1616
diagnose firewall internet-service-cache list	1616
diagnose firewall internet-service-custom	1616
diagnose firewall internet-service-custom list	1617
diagnose firewall internet-service-disable	1617
diagnose firewall internet-service-disable list	1617
diagnose firewall internet-service-extension	1617
diagnose firewall internet-service-extension list	1617
diagnose firewall internet-service-prio-id	1618
diagnose firewall internet-service-prio-id list	1618
diagnose firewall internet-service6	1618
diagnose firewall internet-service6 list	1618
diagnose firewall internet-service6-cache	1618
diagnose firewall internet-service6-cache list	1618
diagnose firewall internet-service6-custom	1619
diagnose firewall internet-service6-custom list	1619
diagnose firewall internet-service6-disable	1619
diagnose firewall internet-service6-disable list	1619
diagnose firewall internet-service6-extension	1619
diagnose firewall internet-service6-extension list	1620
diagnose firewall internet-service6-prio-id	1620
diagnose firewall internet-service6-prio-id list	1620
diagnose firewall ipgeo	1620
diagnose firewall ipgeo copyright-notice	1620
diagnose firewall ipgeo country-list	1620
diagnose firewall ipgeo ip-list	1621
diagnose firewall ipgeo ip2country	1621
diagnose firewall ipgeo override	1621
diagnose firewall network-service-dynamic	1621
diagnose firewall network-service-dynamic list	1621
diagnose firewall nslookup	1622
diagnose firewall shaper	1622
diagnose firewall shaper per-ip-shaper	1622
diagnose firewall shaper per-ip-shaper clear	1622
diagnose firewall shaper per-ip-shaper list	1622
diagnose firewall shaper per-ip-shaper state	1622
diagnose firewall shaper per-ip-shaper stats	1623
diagnose firewall shaper traffic-shaper	1623
diagnose firewall shaper traffic-shaper list	1623
diagnose firewall shaper traffic-shaper stats	1623

diagnose firewall shaper traffic-shaper stats clear	1623
diagnose firewall shaper traffic-shaper stats list	1623
diagnose firewall snat-ippool	1624
diagnose firewall snat-ippool list	1624
diagnose firewall snat-ippool list6	1624
diagnose fortiguard-resources	1624
diagnose fortiguard-resources delete	1626
diagnose fortiguard-resources delete app-categories	1626
diagnose fortiguard-resources delete app-info	1626
diagnose fortiguard-resources delete dlp-object	1626
diagnose fortiguard-resources delete fortiap-end-of-support	1627
diagnose fortiguard-resources delete fortixtender-end-of-support	1627
diagnose fortiguard-resources delete fortigate-end-of-support	1627
diagnose fortiguard-resources delete fortiswitch-end-of-support	1627
diagnose fortiguard-resources delete ips-information	1627
diagnose fortiguard-resources delete prefix-links	1628
diagnose fortiguard-resources delete sprite-casb	1628
diagnose fortiguard-resources delete sprite-isdb	1628
diagnose fortiguard-resources delete sprite-map	1628
diagnose fortiguard-resources delete static-links	1628
diagnose fortiguard-resources delete wf-categories	1628
diagnose fortiguard-resources delete-all	1629
diagnose fortiguard-resources downloads	1629
diagnose fortiguard-resources downloads disable	1629
diagnose fortiguard-resources downloads enable	1629
diagnose fortiguard-resources info	1629
diagnose fortiguard-resources info app-categories	1629
diagnose fortiguard-resources info app-info	1630
diagnose fortiguard-resources info dlp-object	1630
diagnose fortiguard-resources info fortiap-end-of-support	1630
diagnose fortiguard-resources info fortixtender-end-of-support	1630
diagnose fortiguard-resources info fortigate-end-of-support	1630
diagnose fortiguard-resources info fortiswitch-end-of-support	1631
diagnose fortiguard-resources info ips-information	1631
diagnose fortiguard-resources info prefix-links	1631
diagnose fortiguard-resources info sprite-casb.css	1631
diagnose fortiguard-resources info sprite-casb.png	1631
diagnose fortiguard-resources info sprite-isdb.css	1631
diagnose fortiguard-resources info sprite-isdb.png	1632
diagnose fortiguard-resources info sprite-map.css	1632
diagnose fortiguard-resources info sprite-map.png	1632
diagnose fortiguard-resources info static-links	1632
diagnose fortiguard-resources info wf-categories	1632
diagnose fortiguard-resources log	1632
diagnose fortiguard-resources log all	1633
diagnose fortiguard-resources log app-categories	1633
diagnose fortiguard-resources log app-info	1633
diagnose fortiguard-resources log fortiap-end-of-support	1633
diagnose fortiguard-resources log fortixtender-end-of-support	1633

diagnose fortiguard-resources log fortigate-end-of-support	1633
diagnose fortiguard-resources log fortiswitch-end-of-support	1634
diagnose fortiguard-resources log ips-information	1634
diagnose fortiguard-resources log maintainer	1634
diagnose fortiguard-resources log prefix-links	1634
diagnose fortiguard-resources log sprite-casb	1634
diagnose fortiguard-resources log sprite-isdb	1634
diagnose fortiguard-resources log sprite-map	1635
diagnose fortiguard-resources log static-links	1635
diagnose fortiguard-resources log wf-categories	1635
diagnose fortiguard-resources update	1635
diagnose fortiguard-resources update app-categories	1635
diagnose fortiguard-resources update app-info	1635
diagnose fortiguard-resources update dlp-object	1636
diagnose fortiguard-resources update fortiap-end-of-support	1636
diagnose fortiguard-resources update fortixtender-end-of-support	1636
diagnose fortiguard-resources update fortigate-end-of-support	1636
diagnose fortiguard-resources update fortiswitch-end-of-support	1636
diagnose fortiguard-resources update ips-information	1637
diagnose fortiguard-resources update prefix-links	1637
diagnose fortiguard-resources update sprite-casb	1637
diagnose fortiguard-resources update sprite-isdb	1637
diagnose fortiguard-resources update sprite-map	1637
diagnose fortiguard-resources update static-links	1637
diagnose fortiguard-resources update wf-categories	1638
diagnose fortitoken	1638
diagnose fortitoken debug	1638
diagnose fortitoken debug disable	1638
diagnose fortitoken debug enable	1638
diagnose fortitoken info	1638
diagnose fortitoken test	1639
diagnose fortitoken-cloud	1639
diagnose fortitoken-cloud clear	1640
diagnose fortitoken-cloud debug	1640
diagnose fortitoken-cloud debug disable	1640
diagnose fortitoken-cloud debug enable	1640
diagnose fortitoken-cloud debug info	1640
diagnose fortitoken-cloud delete	1640
diagnose fortitoken-cloud migrate-ftm	1641
diagnose fortitoken-cloud server	1641
diagnose fortitoken-cloud set-http	1641
diagnose fortitoken-cloud show	1641
diagnose fortitoken-cloud sync	1642
diagnose fortitoken-cloud update	1642
diagnose fortiview	1642
diagnose fortiview device	1642
diagnose fortiview result	1643
diagnose fortiview shaper-stats	1643
diagnose fortiview sortby	1643

diagnose fortiview time	1643
diagnose fortiview view	1643
diagnose geoip	1643
diagnose geoip delete-geoip-db	1644
diagnose geoip geoip-query	1644
diagnose geoip ip2country	1644
diagnose geoip iprange	1644
diagnose geoip iprange6	1644
diagnose hardware	1645
diagnose hardware certificate	1645
diagnose hardware deviceinfo	1645
diagnose hardware deviceinfo disk	1646
diagnose hardware deviceinfo nic	1646
diagnose hardware deviceinfo nic-channel	1646
diagnose hardware deviceinfo nic-stats	1646
diagnose hardware deviceinfo tpm	1646
diagnose hardware getcbp	1646
diagnose hardware ioport	1647
diagnose hardware lspci	1647
diagnose hardware mii	1647
diagnose hardware setcbp	1647
diagnose hardware setpci	1647
diagnose hardware sysinfo	1647
diagnose hardware sysinfo conserve	1648
diagnose hardware sysinfo cpu	1648
diagnose hardware sysinfo interrupts	1648
diagnose hardware sysinfo iomem	1648
diagnose hardware sysinfo ioports	1648
diagnose hardware sysinfo memory	1648
diagnose hardware sysinfo mtrr	1649
diagnose hardware sysinfo slab	1649
diagnose http-view	1649
diagnose http-view clear	1649
diagnose http-view debug	1649
diagnose http-view log-show	1650
diagnose http-view restart	1650
diagnose http-view stats	1650
diagnose ip	1650
diagnose ip address	1651
diagnose ip address add	1651
diagnose ip address delete	1651
diagnose ip address list	1652
diagnose ip arp	1652
diagnose ip arp add	1652
diagnose ip arp delete	1652
diagnose ip arp list	1652
diagnose ip parp	1653
diagnose ip parp list	1653
diagnose ip route	1653

diagnose ip route add	1653
diagnose ip route delete	1653
diagnose ip route list	1654
diagnose ip route match	1654
diagnose ip route verify	1654
diagnose ip tcp	1654
diagnose ip tcp list	1654
diagnose ip udp	1655
diagnose ip udp list	1655
diagnose ip address	1655
diagnose ip address add	1655
diagnose ip address delete	1655
diagnose ip address list	1656
diagnose ip arp	1656
diagnose ip arp add	1656
diagnose ip arp delete	1656
diagnose ip arp list	1657
diagnose ip parp	1657
diagnose ip parp list	1657
diagnose ip route	1657
diagnose ip route add	1658
diagnose ip route delete	1658
diagnose ip route list	1658
diagnose ip route match	1658
diagnose ip route verify	1658
diagnose ip tcp	1659
diagnose ip tcp list	1659
diagnose ip udp	1659
diagnose ip udp list	1659
diagnose ipsec	1659
diagnose ipsec connect	1660
diagnose ipsec list-conn	1660
diagnose ipsec list-sa	1660
diagnose ipsec p1-status	1660
diagnose ipsec reload-ca	1660
diagnose ipsec reload-ipsec	1661
diagnose ipset	1661
diagnose ipset list	1661
diagnose iptables	1661
diagnose iptables dry-run	1661
diagnose iptables list	1662
diagnose iptables list6	1662
diagnose iptables refresh	1662
diagnose iptables shaper	1662
diagnose iptables shaper-stats	1662
diagnose ipv6	1662
diagnose ipv6 address	1663
diagnose ipv6 address add	1663

diagnose ipv6 address delete	1663
diagnose ipv6 address list	1664
diagnose ipv6 devconf	1664
diagnose ipv6 devconf accept-dad	1664
diagnose ipv6 devconf disable_ipv6	1664
diagnose ipv6 neighbor-cache	1664
diagnose ipv6 neighbor-cache add	1665
diagnose ipv6 neighbor-cache delete	1665
diagnose ipv6 neighbor-cache flush	1665
diagnose ipv6 neighbor-cache list	1665
diagnose ipv6 route	1666
diagnose ipv6 route list	1666
diagnose ipv6 address	1666
diagnose ipv6 address add	1666
diagnose ipv6 address delete	1666
diagnose ipv6 address list	1667
diagnose ipv6 neighbor-cache	1667
diagnose ipv6 neighbor-cache add	1667
diagnose ipv6 neighbor-cache delete	1667
diagnose ipv6 neighbor-cache flush	1668
diagnose ipv6 neighbor-cache list	1668
diagnose ipv6 route	1668
diagnose ipv6 route list	1668
diagnose lldprx	1668
diagnose lldprx config	1669
diagnose lldprx neighbor	1669
diagnose lldprx neighbor clear	1669
diagnose lldprx neighbor details	1670
diagnose lldprx neighbor summary	1670
diagnose lldprx port	1670
diagnose lldprx port details	1670
diagnose lldprx port neighbor	1670
diagnose lldprx port neighbor clear	1670
diagnose lldprx port neighbor details	1671
diagnose lldprx port neighbor summary	1671
diagnose lldprx port summary	1671
diagnose lldprx restart	1671
diagnose lldprx stats	1671
diagnose lldprx stats config	1671
diagnose lldprx stats crash	1672
diagnose lldprx stats manager	1672
diagnose lldprx stats scan	1672
diagnose log	1672
diagnose log alertmail	1673
diagnose log alertmail authcode	1673
diagnose log alertmail test	1673
diagnose log check-empty	1673
diagnose log clear-kernel-stats	1673
diagnose log dummy-log	1674

diagnose log dummy-log fill	1674
diagnose log dummy-log remove	1674
diagnose log field-enum	1674
diagnose log field-list	1674
diagnose log kernel-stats	1674
diagnose log severity	1675
diagnose log show	1675
diagnose log stress-test	1675
diagnose log sub-category	1675
diagnose log test	1675
diagnose log test-text	1675
diagnose netlink	1676
diagnose netlink backlog	1676
diagnose netlink backlog get	1676
diagnose netlink backlog set	1677
diagnose netlink brctl	1677
diagnose netlink brctl forward-domain-status	1677
diagnose netlink brctl interface-stats	1677
diagnose netlink brctl list	1677
diagnose netlink brctl name	1677
diagnose netlink brctl vlan-filt-conf	1678
diagnose netlink device	1678
diagnose netlink device list	1678
diagnose netlink interface	1678
diagnose netlink interface clear	1678
diagnose netlink interface list	1679
diagnose netlink interface packet-rate	1679
diagnose netlink interface speed-test	1679
diagnose netlink interface speed-test-result	1679
diagnose netlink interface speed-test-result-clear	1679
diagnose netlink intf-class	1680
diagnose netlink intf-class list	1680
diagnose netlink intf-qdisc	1680
diagnose netlink intf-qdisc list	1680
diagnose netlink qlen	1680
diagnose netlink qlen get	1681
diagnose netlink qlen set	1681
diagnose nodejs	1681
diagnose nodejs health-check	1682
diagnose nodejs health-check ping	1682
diagnose nodejs logs	1682
diagnose nodejs logs delete	1682
diagnose nodejs logs list	1682
diagnose nodejs logs show	1682
diagnose nodejs logs show-all	1683
diagnose nodejs performance	1683
diagnose nodejs performance mass-ztna-event-logs	1683
diagnose nodejs process	1683
diagnose nodejs process restart	1683

diagnose oci	1684
diagnose oci pubkey	1684
diagnose on-demand-sniffer	1684
diagnose on-demand-sniffer delete-results	1684
diagnose on-demand-sniffer list	1685
diagnose on-demand-sniffer start	1685
diagnose on-demand-sniffer stop	1685
diagnose preload	1685
diagnose preload clear	1686
diagnose preload debug	1686
diagnose preload log-show	1686
diagnose preload restart	1686
diagnose preload stats	1686
diagnose report	1687
diagnose report clear-filter	1687
diagnose report dataset	1687
diagnose report filter	1687
diagnose report min-points	1687
diagnose report ondemand-table	1688
diagnose report sql	1688
diagnose report time	1688
diagnose report top-n	1688
diagnose report-runner	1688
diagnose report-runner clean	1688
diagnose report-runner trigger	1689
diagnose report-runner trigger security-rating-reports	1689
diagnose report-runner vuln-clean	1689
diagnose report-runner vuln-read	1689
diagnose report-runner-v2	1689
diagnose report-runner-v2 security-rating	1690
diagnose report-runner-v2 security-rating clean	1690
diagnose report-runner-v2 security-rating reset-trigger	1690
diagnose saas	1690
diagnose saas reload	1690
diagnose saas show	1690
diagnose saas show apps	1691
diagnose saas show details	1691
diagnose saas show status	1691
diagnose settings	1691
diagnose settings info	1691
diagnose settings reset	1691
diagnose sniffer	1692
diagnose sniffer migsock	1692
diagnose sniffer migsock debug-trace	1692
diagnose sniffer migsock debug-trace disable	1692
diagnose sniffer migsock debug-trace enable	1693
diagnose sniffer migsock filter	1693
diagnose sniffer migsock ssl-trace	1693

diagnose sniffer migsock ssl-trace disable	1693
diagnose sniffer migsock ssl-trace enable	1693
diagnose sniffer migsock start	1693
diagnose sniffer migsock timestamp	1694
diagnose sniffer migsock timestamp disable	1694
diagnose sniffer migsock timestamp enable	1694
diagnose sniffer packet	1694
diagnose snmp	1695
diagnose snmp ip	1695
diagnose snmp ip frags	1696
diagnose snmp ip icmp	1696
diagnose snmp ip tcp	1696
diagnose snmp ip udp	1696
diagnose snmp ip6	1696
diagnose snmp ip6 frags	1697
diagnose snmp ip6 icmp6	1697
diagnose snmp ip6 udp6	1697
diagnose snmp net	1697
diagnose snmp net stat	1697
diagnose snmp trap	1698
diagnose snmp trap send	1698
diagnose sys	1698
diagnose sys botnet-domain	1709
diagnose sys botnet-domain hit	1709
diagnose sys botnet-domain list	1710
diagnose sys botnet-ip	1710
diagnose sys botnet-ip find	1710
diagnose sys botnet-ip flush	1710
diagnose sys botnet-ip hit	1710
diagnose sys botnet-ip list	1710
diagnose sys cmdb	1711
diagnose sys cmdb check-lock	1711
diagnose sys cmdb dump	1711
diagnose sys cmdb dump vdom	1711
diagnose sys cmdb flag	1711
diagnose sys cmdb flag info	1712
diagnose sys cmdb flag reset	1712
diagnose sys cmdb flag reset script-running	1712
diagnose sys cmdb info	1712
diagnose sys cmdb obj-verno	1712
diagnose sys cmdb refcnt	1712
diagnose sys cmdb refcnt reset	1713
diagnose sys cmdb refcnt show	1713
diagnose sys cmdb set-readlock	1713
diagnose sys cmdb unset-readlock	1713
diagnose sys cmdb-profile	1713
diagnose sys cmdb-profile info	1714
diagnose sys cmdb-profile node	1714
diagnose sys cmdb-profile reset	1714

diagnose sys cmdb-profile top10	1714
diagnose sys cmdb-profile top10 average	1714
diagnose sys cmdb-profile top10 total	1715
diagnose sys config-transaction	1715
diagnose sys config-transaction show	1715
diagnose sys config-transaction show entity-by-txn	1715
diagnose sys config-transaction show mctx	1715
diagnose sys config-transaction show txn-cli-commands	1716
diagnose sys config-transaction show txn-entity	1716
diagnose sys config-transaction show txn-info	1716
diagnose sys config-transaction show txn-lock	1716
diagnose sys config-transaction show txn-meta	1716
diagnose sys config-transaction status	1716
diagnose sys contrack	1717
diagnose sys contrack clear	1717
diagnose sys contrack count	1717
diagnose sys contrack list-dying4	1717
diagnose sys contrack list-dying6	1717
diagnose sys contrack list-unconfirmed4	1717
diagnose sys contrack list-unconfirmed6	1718
diagnose sys contrack list4	1718
diagnose sys contrack list6	1718
diagnose sys contrack stats	1718
diagnose sys csf	1718
diagnose sys csf authorization	1718
diagnose sys csf authorization accept	1719
diagnose sys csf authorization deny	1719
diagnose sys csf authorization pending-list	1719
diagnose sys csf downstream	1719
diagnose sys csf downstream-devices	1720
diagnose sys csf dynamic-sync-read	1720
diagnose sys csf dynamic-sync-request	1720
diagnose sys csf dynamic-sync-update	1720
diagnose sys csf fabric-device	1721
diagnose sys csf fabric-device list	1721
diagnose sys csf file	1721
diagnose sys csf file cat	1721
diagnose sys csf file top-mem	1721
diagnose sys csf forticloud-id-list	1722
diagnose sys csf get-bulk-global-view	1722
diagnose sys csf global	1722
diagnose sys csf initialize-cmd	1722
diagnose sys csf license	1722
diagnose sys csf merge-cmd	1723
diagnose sys csf neighbor	1723
diagnose sys csf neighbor flush	1723
diagnose sys csf neighbor list	1723
diagnose sys csf query	1724
diagnose sys csf ratelimit-test-sender	1724

diagnose sys csf ratelimit-test-server	1724
diagnose sys csf send-test-log-upstream	1724
diagnose sys csf seqpacket-message-listener	1725
diagnose sys csf seqpacket-message-sender	1725
diagnose sys csf stream-message-listener	1725
diagnose sys csf stream-message-sender	1725
diagnose sys csf tunnel-test-listener	1726
diagnose sys csf tunnel-test-sender	1726
diagnose sys csf upstream	1726
diagnose sys csf versions	1726
diagnose sys dayst-info	1726
diagnose sys device	1727
diagnose sys device add	1727
diagnose sys device delete	1727
diagnose sys device list	1727
diagnose sys external-resource	1728
diagnose sys external-resource list	1728
diagnose sys external-resource push-add	1728
diagnose sys external-resource push-api-json-commands	1728
diagnose sys external-resource push-remove	1728
diagnose sys external-resource push-snapshot	1729
diagnose sys external-resource stats	1729
diagnose sys fips	1729
diagnose sys fips error-mode	1729
diagnose sys fips kat-error	1729
diagnose sys forticonverter	1730
diagnose sys forticonverter available-source-devices	1730
diagnose sys forticonverter create-ticket	1730
diagnose sys forticonverter custom-create-ticket	1730
diagnose sys forticonverter download-status	1730
diagnose sys forticonverter eligibility-status	1731
diagnose sys forticonverter get-prompt-visibility	1731
diagnose sys forticonverter result-availability	1731
diagnose sys forticonverter set-source-fortigate	1731
diagnose sys forticonverter source-config-upload-status	1732
diagnose sys forticonverter source-interfaces	1732
diagnose sys forticonverter start-download	1732
diagnose sys forticonverter submitted-info	1732
diagnose sys forticonverter update-eligibility	1733
diagnose sys forticonverter update-result-availability	1733
diagnose sys forticonverter upload-local-config	1733
diagnose sys forticonverter upload-status	1733
diagnose sys ha	1733
diagnose sys ha check-vc	1734
diagnose sys ha checksum	1734
diagnose sys ha checksum cached	1734
diagnose sys ha checksum cluster	1734
diagnose sys ha checksum log	1734
diagnose sys ha checksum log clear	1734

diagnose sys ha checksum log disable	1735
diagnose sys ha checksum log enable	1735
diagnose sys ha checksum recalculate	1735
diagnose sys ha checksum show	1735
diagnose sys ha checksum show-nonsync	1736
diagnose sys ha checksum test	1736
diagnose sys ha dump-by	1736
diagnose sys ha dump-by debug-zone	1736
diagnose sys ha dump-by device	1736
diagnose sys ha dump-by group	1736
diagnose sys ha dump-by kernel	1737
diagnose sys ha dump-by rcache	1737
diagnose sys ha dump-by vcluster	1737
diagnose sys ha dump-by vdom	1737
diagnose sys ha extfile-sig	1737
diagnose sys ha fgsp-zone	1737
diagnose sys ha fib	1738
diagnose sys ha hactx-stats	1738
diagnose sys ha hactx-stats clear	1738
diagnose sys ha hadiff	1738
diagnose sys ha hadiff log	1738
diagnose sys ha hadiff log clear	1738
diagnose sys ha hadiff log disable	1739
diagnose sys ha hadiff log enable	1739
diagnose sys ha hadiff max-sync-turns	1739
diagnose sys ha hadiff max-unsync-wait	1739
diagnose sys ha hadiff status	1739
diagnose sys ha hadiff sync-from-higher	1740
diagnose sys ha hasync-conn-max-buf	1740
diagnose sys ha hasync-stats	1740
diagnose sys ha hasync-stats all	1740
diagnose sys ha hasync-stats by-object	1740
diagnose sys ha hasync-stats most-recent	1741
diagnose sys ha hasync-stats most-time	1741
diagnose sys ha heartbeat	1741
diagnose sys ha history	1741
diagnose sys ha history clear	1741
diagnose sys ha history read	1742
diagnose sys ha mac	1742
diagnose sys ha pingsvr-secondary-force-reset	1742
diagnose sys ha recalculate-extfile-signature	1742
diagnose sys ha reset-health-status	1742
diagnose sys ha reset-uptime	1742
diagnose sys ha reset-uptime-primary-only	1743
diagnose sys ha session-sync-dev	1743
diagnose sys ha session-sync-dev clear	1743
diagnose sys ha session-sync-dev set	1743
diagnose sys ha standalone-peers	1743
diagnose sys ha standalone-peers reset-stats	1743

diagnose sys ha stats	1744
diagnose sys ha status	1744
diagnose sys ha sync-stats	1744
diagnose sys ha sync-stats-reset	1744
diagnose sys ha vlan-hb-monitor	1744
diagnose sys icap-remote-server	1744
diagnose sys icap-remote-server status	1745
diagnose sys iotop	1745
diagnose sys link-monitor	1745
diagnose sys link-monitor filter	1745
diagnose sys link-monitor filter clear	1745
diagnose sys link-monitor filter name	1745
diagnose sys link-monitor interface	1746
diagnose sys link-monitor launch	1746
diagnose sys link-monitor reset-monitor	1746
diagnose sys link-monitor sdwan-hc	1746
diagnose sys link-monitor sdwan-service	1747
diagnose sys link-monitor shm-band-stats	1747
diagnose sys link-monitor shm-stats	1747
diagnose sys link-monitor status	1747
diagnose sys nmi-watchdog	1748
diagnose sys nmi-watchdog disable	1748
diagnose sys nmi-watchdog enable	1748
diagnose sys nmi-watchdog reboot	1748
diagnose sys nmi-watchdog reboot disable	1748
diagnose sys nmi-watchdog reboot enable	1748
diagnose sys nmi-watchdog threshold	1749
diagnose sys ntp	1749
diagnose sys ntp status	1749
diagnose sys pair	1749
diagnose sys process	1749
diagnose sys process daemon-auto-restart	1749
diagnose sys process dump	1750
diagnose sys process nameof	1750
diagnose sys process pidof	1750
diagnose sys process pstack	1750
diagnose sys process sock-mem	1751
diagnose sys process socket	1751
diagnose sys process trace	1751
diagnose sys profile	1751
diagnose sys profile cpumask	1751
diagnose sys profile show	1752
diagnose sys profile show detail	1752
diagnose sys profile show order	1752
diagnose sys profile start	1752
diagnose sys profile step	1752
diagnose sys profile stop	1752
diagnose sys profile sysmap	1753
diagnose sys ptp	1753

diagnose sys ptp status	1753
diagnose sys scanunit	1753
diagnose sys scanunit auto-restart	1753
diagnose sys scanunit auto-restart requests	1753
diagnose sys scanunit auto-restart reset	1754
diagnose sys scanunit auto-restart status	1754
diagnose sys scanunit auto-restart time	1754
diagnose sys scanunit av-filetype-reuse	1754
diagnose sys scanunit av-filetype-reuse disable	1754
diagnose sys scanunit av-filetype-reuse enable	1754
diagnose sys scanunit bypass	1755
diagnose sys scanunit bypass clear	1755
diagnose sys scanunit bypass disable	1755
diagnose sys scanunit bypass disable category	1755
diagnose sys scanunit bypass disable category all	1755
diagnose sys scanunit bypass disable category av-engine	1755
diagnose sys scanunit bypass disable category scanunit	1756
diagnose sys scanunit bypass disable protocol	1756
diagnose sys scanunit bypass disable protocol all	1756
diagnose sys scanunit bypass disable protocol cifs	1756
diagnose sys scanunit bypass disable protocol ftp	1756
diagnose sys scanunit bypass disable protocol http	1756
diagnose sys scanunit bypass disable protocol imap	1757
diagnose sys scanunit bypass disable protocol nntp	1757
diagnose sys scanunit bypass disable protocol pop3	1757
diagnose sys scanunit bypass disable protocol smtp	1757
diagnose sys scanunit bypass enable	1757
diagnose sys scanunit bypass enable category	1757
diagnose sys scanunit bypass enable category all	1758
diagnose sys scanunit bypass enable category av-engine	1758
diagnose sys scanunit bypass enable category scanunit	1758
diagnose sys scanunit bypass enable protocol	1758
diagnose sys scanunit bypass enable protocol all	1758
diagnose sys scanunit bypass enable protocol cifs	1758
diagnose sys scanunit bypass enable protocol ftp	1759
diagnose sys scanunit bypass enable protocol http	1759
diagnose sys scanunit bypass enable protocol imap	1759
diagnose sys scanunit bypass enable protocol nntp	1759
diagnose sys scanunit bypass enable protocol pop3	1759
diagnose sys scanunit bypass enable protocol smtp	1759
diagnose sys scanunit bypass show	1760
diagnose sys scanunit cfg	1760
diagnose sys scanunit cfg clear	1760
diagnose sys scanunit cfg list	1760
diagnose sys scanunit crash-dump	1760
diagnose sys scanunit crash-dump clear	1760
diagnose sys scanunit crash-dump disable	1761
diagnose sys scanunit crash-dump enable	1761
diagnose sys scanunit crash-dump read	1761

diagnose sys scanunit debug	1761
diagnose sys scanunit debug all	1761
diagnose sys scanunit debug analytics	1761
diagnose sys scanunit debug antisipam	1762
diagnose sys scanunit debug daemon	1762
diagnose sys scanunit debug dlp	1762
diagnose sys scanunit debug file-filter	1762
diagnose sys scanunit debug ia	1763
diagnose sys scanunit debug icb	1763
diagnose sys scanunit debug job	1763
diagnose sys scanunit debug level	1763
diagnose sys scanunit debug level error	1763
diagnose sys scanunit debug level info	1764
diagnose sys scanunit debug level verbose	1764
diagnose sys scanunit debug level warning	1764
diagnose sys scanunit debug outbreak-prevention	1764
diagnose sys scanunit debug quarantine	1764
diagnose sys scanunit debug reset	1765
diagnose sys scanunit debug sane	1765
diagnose sys scanunit debug show	1765
diagnose sys scanunit dlp	1765
diagnose sys scanunit dlp reset	1765
diagnose sys scanunit dlp status	1765
diagnose sys scanunit dlp threshold	1766
diagnose sys scanunit file-hash	1766
diagnose sys scanunit file-hash list	1766
diagnose sys scanunit file-hash list all	1766
diagnose sys scanunit file-hash list md5	1766
diagnose sys scanunit file-hash list sha1	1766
diagnose sys scanunit file-hash list sha256	1767
diagnose sys scanunit file-hash query	1767
diagnose sys scanunit file-hash query md5	1767
diagnose sys scanunit file-hash query sha1	1767
diagnose sys scanunit file-hash query sha256	1767
diagnose sys scanunit file-hash status	1768
diagnose sys scanunit filter	1768
diagnose sys scanunit filter clear	1768
diagnose sys scanunit filter list	1768
diagnose sys scanunit filter negate	1768
diagnose sys scanunit filter negate vd	1768
diagnose sys scanunit filter negate worker	1769
diagnose sys scanunit filter vd	1769
diagnose sys scanunit filter worker	1769
diagnose sys scanunit log	1769
diagnose sys scanunit log filter	1769
diagnose sys scanunit log filter clear	1770
diagnose sys scanunit log filter list	1770
diagnose sys scanunit log filter negate	1770
diagnose sys scanunit log filter negate vd	1770

diagnose sys scanunit log filter negate worker	1770
diagnose sys scanunit log filter vd	1770
diagnose sys scanunit log filter worker	1771
diagnose sys scanunit memory	1771
diagnose sys scanunit memory conserve	1771
diagnose sys scanunit memory conserve enter	1771
diagnose sys scanunit memory conserve exit	1771
diagnose sys scanunit reload-avdb	1771
diagnose sys scanunit reload-aveng	1772
diagnose sys scanunit reload-fsa-ext	1772
diagnose sys scanunit restart	1772
diagnose sys scanunit simulate-crash	1772
diagnose sys scanunit simulate-crash lockup-workers	1772
diagnose sys scanunit simulate-crash lockup-workers all	1772
diagnose sys scanunit simulate-crash lockup-workers worker	1773
diagnose sys scanunit simulate-error	1773
diagnose sys scanunit simulate-error av-engine-delay	1773
diagnose sys scanunit simulate-error av-error	1773
diagnose sys scanunit simulate-error av-status	1773
diagnose sys scanunit simulate-error cdr-error	1774
diagnose sys scanunit simulate-error reset	1774
diagnose sys scanunit simulate-error scan-error-code	1774
diagnose sys scanunit simulate-error status	1774
diagnose sys scanunit stats	1774
diagnose sys scanunit stats all	1775
diagnose sys scanunit stats clear	1775
diagnose sys scanunit stats crash	1775
diagnose sys scanunit stats forker	1775
diagnose sys scanunit stats list	1775
diagnose sys scanunit stats manager	1775
diagnose sys scanunit stats worker	1776
diagnose sys scanunit valgrind	1776
diagnose sys scanunit valgrind disable	1776
diagnose sys scanunit valgrind enable	1776
diagnose sys scanunit valgrind log	1776
diagnose sys scanunit valgrind log clear	1776
diagnose sys scanunit valgrind log show	1777
diagnose sys scanunit valgrind memcheck	1777
diagnose sys scanunit valgrind memcheck_less	1777
diagnose sys scanunit valgrind status	1777
diagnose sys scanunit vdom-stats	1777
diagnose sys scanunit vdom-stats all	1777
diagnose sys scanunit vdom-stats clear	1778
diagnose sys scanunit vdom-stats clear-all	1778
diagnose sys scanunit vdom-stats list	1778
diagnose sys scanunit watchdog-override	1778
diagnose sys scanunit watchdog-override disable	1778
diagnose sys scanunit watchdog-override enable	1778
diagnose sys scanunit watchdog-override interval	1779

diagnose sys sdn	1779
diagnose sys sdn cache	1779
diagnose sys sdn status	1779
diagnose sys server-probe	1780
diagnose sys server-probe response	1780
diagnose sys session	1780
diagnose sys session clear	1780
diagnose sys session count	1780
diagnose sys session exp-stat	1780
diagnose sys session expectation	1781
diagnose sys session filter	1781
diagnose sys session filter clear	1781
diagnose sys session filter clear dintf	1781
diagnose sys session filter clear dport	1781
diagnose sys session filter clear dst	1781
diagnose sys session filter clear nsrc	1782
diagnose sys session filter clear policy	1782
diagnose sys session filter clear proto	1782
diagnose sys session filter clear proto-state	1782
diagnose sys session filter clear sintf	1782
diagnose sys session filter clear sport	1782
diagnose sys session filter clear src	1783
diagnose sys session filter dintf	1783
diagnose sys session filter dport	1783
diagnose sys session filter dst	1783
diagnose sys session filter nsrc	1783
diagnose sys session filter policy	1784
diagnose sys session filter proto	1784
diagnose sys session filter sintf	1784
diagnose sys session filter sport	1784
diagnose sys session filter src	1785
diagnose sys session full-stat	1785
diagnose sys session list	1785
diagnose sys session stat	1785
diagnose sys session ttl	1785
diagnose sys session6	1785
diagnose sys session6 clear	1786
diagnose sys session6 expectation	1786
diagnose sys session6 filter	1786
diagnose sys session6 filter clear	1786
diagnose sys session6 filter clear dintf	1786
diagnose sys session6 filter clear dport	1786
diagnose sys session6 filter clear dst	1787
diagnose sys session6 filter clear nsrc	1787
diagnose sys session6 filter clear policy	1787
diagnose sys session6 filter clear proto	1787
diagnose sys session6 filter clear proto-state	1787
diagnose sys session6 filter clear sintf	1787
diagnose sys session6 filter clear sport	1788

diagnose sys session6 filter clear src	1788
diagnose sys session6 filter clear vd	1788
diagnose sys session6 filter dintf	1788
diagnose sys session6 filter dport	1788
diagnose sys session6 filter dst	1789
diagnose sys session6 filter nsrc	1789
diagnose sys session6 filter policy	1789
diagnose sys session6 filter proto	1789
diagnose sys session6 filter sintf	1789
diagnose sys session6 filter sport	1790
diagnose sys session6 filter src	1790
diagnose sys session6 list	1790
diagnose sys shmfile	1790
diagnose sys shmfile dump	1790
diagnose sys shmfile dump oid-app	1791
diagnose sys shmfile dump oid-slab	1791
diagnose sys shmfile dump slab-file	1791
diagnose sys shmfile dump table-count	1791
diagnose sys shmfile dump table-count total	1791
diagnose sys shmfile dump table-count vdom	1792
diagnose sys shmfile dump vdom	1792
diagnose sys tcp-option	1792
diagnose sys tcp-option disable	1792
diagnose sys tcp-option dump	1793
diagnose sys tcp-option enable	1793
diagnose sys tcpsock	1793
diagnose sys tcpsock6	1793
diagnose sys top	1793
diagnose sys top-all	1794
diagnose sys top-fd	1794
diagnose sys top-fd detail	1794
diagnose sys top-mem	1794
diagnose sys top-mem detail	1795
diagnose sys top-sockmem	1795
diagnose sys traffic	1795
diagnose sys traffic app-stats	1795
diagnose sys traffic app-stats list	1796
diagnose sys udpsock	1796
diagnose sys udpsock6	1796
diagnose sys uuid	1796
diagnose sys uuid allow-manual-set	1796
diagnose sys uuid allow-manual-set disable	1796
diagnose sys uuid allow-manual-set enable	1797
diagnose sys uuid generate	1797
diagnose sys var-zone	1797
diagnose sys var-zone show	1797
diagnose sys vd	1797
diagnose sys vd add	1797
diagnose sys vd delete	1798

diagnose sys vd list	1798
diagnose sys vd set	1798
diagnose sys vd stats	1798
diagnose sys vlan	1798
diagnose sys vlan list	1799
diagnose sys vxlan	1799
diagnose sys vxlan device	1799
diagnose sys vxlan fdb	1799
diagnose sys vxlan fdb list	1799
diagnose test analytics-pdf-report	1799
diagnose test analytics-pdf-report list	1800
diagnose test analytics-pdf-report max	1800
diagnose test analytics-pdf-report request	1800
diagnose test analytics-pdf-report status	1800
diagnose test analytics-report	1800
diagnose test analytics-report checksum	1801
diagnose test application	1801
diagnose test application acd	1803
diagnose test application acsd	1803
diagnose test application autod	1803
diagnose test application awsd	1803
diagnose test application azd	1804
diagnose test application bfd	1804
diagnose test application cloudapid	1804
diagnose test application cmdbsvr	1804
diagnose test application csfd	1805
diagnose test application ddnsd	1805
diagnose test application dhcp6c	1805
diagnose test application dhcp6r	1805
diagnose test application dhcprelay	1805
diagnose test application dlpfingerprint	1806
diagnose test application dlpfpcache	1806
diagnose test application dnsproxy	1806
diagnose test application dsd	1806
diagnose test application eap_supp	1807
diagnose test application evpn	1807
diagnose test application fas	1807
diagnose test application fcnacd	1807
diagnose test application fds_notify	1808
diagnose test application fgtlogd	1808
diagnose test application fnbamd	1808
diagnose test application forticldd	1808
diagnose test application forticron	1808
diagnose test application fsd	1809
diagnose test application fsvrd	1809
diagnose test application gcpd	1809
diagnose test application harelay	1809
diagnose test application hasync	1810
diagnose test application hataik	1810

diagnose test application ibmd	1810
diagnose test application imap	1810
diagnose test application init	1811
diagnose test application iotd	1811
diagnose test application ipamd	1811
diagnose test application ipamsd	1811
diagnose test application ipldbd	1811
diagnose test application ipsengine	1812
diagnose test application ipsmonitor	1812
diagnose test application ipsufd	1812
diagnose test application kmipd	1812
diagnose test application kubed	1813
diagnose test application l2tpcd	1813
diagnose test application lnkmttd	1813
diagnose test application locallogd	1813
diagnose test application miglogd	1814
diagnose test application mrd	1814
diagnose test application netxd	1814
diagnose test application nntp	1814
diagnose test application ocid	1814
diagnose test application openstackd	1815
diagnose test application ovrd	1815
diagnose test application pcpd	1815
diagnose test application pop3	1815
diagnose test application pptpcd	1816
diagnose test application quarantined	1816
diagnose test application radius-das	1816
diagnose test application radiusd	1816
diagnose test application radvd	1817
diagnose test application reportd	1817
diagnose test application sdncd	1817
diagnose test application sdnd	1817
diagnose test application sepmd	1817
diagnose test application sessionsync	1818
diagnose test application sfupgraded	1818
diagnose test application smtp	1818
diagnose test application snmpd	1818
diagnose test application syslogd	1819
diagnose test application updated	1819
diagnose test application uploadd	1819
diagnose test application urlfilter	1819
diagnose test application vned	1820
diagnose test application wad	1820
diagnose test application wccpd	1820
diagnose test application wf_monitor	1820
diagnose test application wiredapd	1820
diagnose test authserver	1821
diagnose test authserver cert	1821
diagnose test authserver ext-idp	1821

diagnose test authserver ldap	1822
diagnose test authserver ldap-digest	1822
diagnose test authserver ldap-direct	1822
diagnose test authserver ldap-search	1822
diagnose test authserver local	1822
diagnose test authserver pop3	1822
diagnose test authserver radius	1823
diagnose test authserver radius-direct	1823
diagnose test authserver tacacs+	1823
diagnose test authserver tacacs+-direct	1823
diagnose test authserver user	1823
diagnose test guest	1823
diagnose test guest add	1824
diagnose test guest del	1824
diagnose test guest list	1824
diagnose test security	1824
diagnose test security mount-invalid-flag	1824
diagnose test security status	1824
diagnose test update	1825
diagnose test update info	1825
diagnose test update tzdb	1825
diagnose tpm	1825
diagnose tpm SHA-1	1825
diagnose tpm SHA-256	1826
diagnose tpm generate-random-number	1826
diagnose tpm get-property	1826
diagnose tpm get-var-property	1826
diagnose tpm read-clock	1826
diagnose tpm selftest	1827
diagnose tpm shutdown-prepare	1827
diagnose traffictest	1827
diagnose traffictest client-intf	1827
diagnose traffictest port	1827
diagnose traffictest proto	1828
diagnose traffictest proto 0	1828
diagnose traffictest proto 1	1828
diagnose traffictest run	1828
diagnose traffictest server-intf	1828
diagnose traffictest show	1829
diagnose user	1829
diagnose user banned-ip	1830
diagnose user banned-ip add	1830
diagnose user banned-ip add src4	1830
diagnose user banned-ip add src6	1831
diagnose user banned-ip clear	1831
diagnose user banned-ip delete	1831
diagnose user banned-ip delete src4	1831
diagnose user banned-ip delete src6	1831

diagnose user banned-ip list	1832
diagnose user banned-ip list all	1832
diagnose user banned-ip list src4	1832
diagnose user banned-ip list src6	1832
diagnose user banned-ip stat	1832
diagnose user banned-ip stress-test	1832
diagnose user device	1833
diagnose user device clear	1833
diagnose user device del	1833
diagnose user device filter	1833
diagnose user device filter addr	1833
diagnose user device filter clear	1834
diagnose user device filter clear addr	1834
diagnose user device filter clear generation	1834
diagnose user device filter clear index	1834
diagnose user device filter clear joined	1834
diagnose user device filter clear vd	1835
diagnose user device filter generation	1835
diagnose user device filter joined	1835
diagnose user device filter list	1835
diagnose user device filter negate	1835
diagnose user device filter negate addr	1836
diagnose user device filter negate generation	1836
diagnose user device filter negate index	1836
diagnose user device filter negate joined	1836
diagnose user device filter negate vd	1836
diagnose user device filter vd	1836
diagnose user device get	1837
diagnose user device list	1837
diagnose user device stats	1837
diagnose user-device-store	1837
diagnose user-device-store device	1839
diagnose user-device-store device fortifone	1839
diagnose user-device-store device fortifone add	1839
diagnose user-device-store device fortifone delete	1839
diagnose user-device-store device fortifone list	1840
diagnose user-device-store device memory	1840
diagnose user-device-store device memory list	1840
diagnose user-device-store device memory mac-host	1840
diagnose user-device-store device memory mac-host add	1840
diagnose user-device-store device memory mac-host filter	1840
diagnose user-device-store device memory mac-host modify	1841
diagnose user-device-store device memory mac-host query	1841
diagnose user-device-store device memory mac-host subscribe	1841
diagnose user-device-store device memory mac-host subscribe disable	1841
diagnose user-device-store device memory mac-host subscribe enable	1841
diagnose user-device-store device memory mac-host validate	1842

diagnose user-device-store device memory ot-purdue-set	1842
diagnose user-device-store device memory query	1842
diagnose user-device-store device memory uid	1842
diagnose user-device-store device memory uid add	1842
diagnose user-device-store device memory uid delete	1842
diagnose user-device-store device memory uid update	1843
diagnose user-device-store device memory vulnerability-detected	1843
diagnose user-device-store device memory vulnerability-query	1843
diagnose user-device-store device memory vulnerability-update	1843
diagnose user-device-store device-stats-query	1843
diagnose user-device-store device-stats-query filters-and	1844
diagnose user-device-store device-stats-query filters-or	1844
diagnose user-device-store email-stats	1844
diagnose user-device-store email-stats list	1844
diagnose user-device-store email-stats query	1844
diagnose user-device-store fsw-device-stats-query	1844
diagnose user-device-store fsw-device-stats-query filters-and	1845
diagnose user-device-store fsw-device-stats-query filters-or	1845
diagnose user-device-store ftcl-device-stats-query	1845
diagnose user-device-store ftcl-device-stats-query filters-and	1845
diagnose user-device-store ftcl-device-stats-query filters-or	1845
diagnose user-device-store iot-ot-vuln	1846
diagnose user-device-store iot-ot-vuln list	1846
diagnose user-device-store iot-ot-vuln query	1846
diagnose user-device-store unified	1846
diagnose user-device-store unified clear	1846
diagnose user-device-store unified debug	1846
diagnose user-device-store unified debug disable	1847
diagnose user-device-store unified debug enable	1847
diagnose user-device-store unified delete	1847
diagnose user-device-store unified device-memory-query	1847
diagnose user-device-store unified device-memory-query filters-and	1847
diagnose user-device-store unified device-memory-query filters-or	1847
diagnose user-device-store unified device-query	1848
diagnose user-device-store unified device-query filters-and	1848
diagnose user-device-store unified device-query filters-or	1848
diagnose user-device-store unified dump	1848
diagnose user-device-store unified list	1848
diagnose user-device-store unified re-query	1848
diagnose user-device-store unified stats	1849
diagnose user-device-store unified user-memory-query	1849
diagnose user-device-store unified user-memory-query filters-and	1849
diagnose user-device-store unified user-memory-query filters-or	1849
diagnose user-device-store unified user-query	1849
diagnose user-device-store unified user-query filters-and	1849
diagnose user-device-store unified user-query filters-or	1850
diagnose user-device-store user	1850
diagnose user-device-store user memory	1850
diagnose user-device-store user memory list	1850

diagnose user-device-store user memory query	1850
diagnose user-device-store user-count	1850
diagnose user-device-store user-count list	1851
diagnose user-device-store user-count query	1851
diagnose user-device-store user-stats	1851
diagnose user-device-store user-stats query	1851
diagnose vendor-mac	1851
diagnose vendor-mac id	1851
diagnose vendor-mac id-summary	1852
diagnose vendor-mac info	1852
diagnose vendor-mac match	1852
diagnose vmware	1852
diagnose vmware ovfenv	1853
diagnose vpn ssl	1853
diagnose wacs	1853
diagnose wacs clear	1853
diagnose wacs restart	1853
diagnose wacs stats	1854
diagnose wad	1854
diagnose wad access-proxy	1867
diagnose wad access-proxy health-check	1867
diagnose wad access-proxy health-check status	1867
diagnose wad config	1868
diagnose wad config auth-rule	1868
diagnose wad config policy	1868
diagnose wad config proxy-policy	1868
diagnose wad config summary	1868
diagnose wad console-log	1868
diagnose wad console-log disable	1869
diagnose wad console-log enable	1869
diagnose wad csvc	1869
diagnose wad csvc bytcache	1869
diagnose wad csvc bytcache clear	1869
diagnose wad csvc bytcache flush	1869
diagnose wad csvc bytcache lists	1870
diagnose wad csvc bytcache stats	1870
diagnose wad csvc bytcache toggle	1870
diagnose wad csvc bytcache toggle all	1870
diagnose wad csvc bytcache toggle create	1871
diagnose wad csvc bytcache toggle read	1871
diagnose wad csvc memcache	1871
diagnose wad csvc memcache clear	1871
diagnose wad csvc memcache flush	1871
diagnose wad csvc memcache lists	1872
diagnose wad csvc memcache stats	1872
diagnose wad csvc restart	1872
diagnose wad csvc webcache	1872
diagnose wad csvc webcache clear	1873
diagnose wad csvc webcache flush	1873

diagnose wad csvc webcache lists	1873
diagnose wad csvc webcache stats	1873
diagnose wad csvc webcache toggle	1873
diagnose wad csvc webcache toggle abort	1874
diagnose wad csvc webcache toggle add_ref	1874
diagnose wad csvc webcache toggle all	1874
diagnose wad csvc webcache toggle append	1874
diagnose wad csvc webcache toggle create	1875
diagnose wad csvc webcache toggle read	1875
diagnose wad csvc webcache toggle remove	1875
diagnose wad csvc webcache toggle resolve	1875
diagnose wad csvc webcache toggle update	1875
diagnose wad debug	1876
diagnose wad debug clear	1876
diagnose wad debug crash	1876
diagnose wad debug crash clear	1876
diagnose wad debug crash disable	1876
diagnose wad debug crash enable	1876
diagnose wad debug crash list	1877
diagnose wad debug crash max	1877
diagnose wad debug crash read	1877
diagnose wad debug disable	1877
diagnose wad debug disable category	1877
diagnose wad debug disable category aio	1878
diagnose wad debug disable category antiphish	1878
diagnose wad debug disable category auth	1878
diagnose wad debug disable category autotest	1878
diagnose wad debug disable category bytecache	1878
diagnose wad debug disable category cache_server	1878
diagnose wad debug disable category casb	1879
diagnose wad debug disable category cifs	1879
diagnose wad debug disable category cmgr	1879
diagnose wad debug disable category config	1879
diagnose wad debug disable category csvc	1879
diagnose wad debug disable category detail	1879
diagnose wad debug disable category devuln	1880
diagnose wad debug disable category diag	1880
diagnose wad debug disable category dispatcher	1880
diagnose wad debug disable category dns	1880
diagnose wad debug disable category dskd	1880
diagnose wad debug disable category email	1880
diagnose wad debug disable category extension	1881
diagnose wad debug disable category ftp	1881
diagnose wad debug disable category http	1881
diagnose wad debug disable category http2	1881
diagnose wad debug disable category http3	1881
diagnose wad debug disable category icap	1881
diagnose wad debug disable category icap_server	1882
diagnose wad debug disable category icbsvc	1882

diagnose wad debug disable category info	1882
diagnose wad debug disable category ips	1882
diagnose wad debug disable category isolator	1882
diagnose wad debug disable category license	1882
diagnose wad debug disable category mapi	1883
diagnose wad debug disable category memblk	1883
diagnose wad debug disable category monitor	1883
diagnose wad debug disable category packet	1883
diagnose wad debug disable category policy	1883
diagnose wad debug disable category policy_test	1883
diagnose wad debug disable category proc	1884
diagnose wad debug disable category quic	1884
diagnose wad debug disable category quic_cc	1884
diagnose wad debug disable category rev_conn	1884
diagnose wad debug disable category rpc	1884
diagnose wad debug disable category scan	1884
diagnose wad debug disable category scp	1885
diagnose wad debug disable category session	1885
diagnose wad debug disable category sftp	1885
diagnose wad debug disable category socks	1885
diagnose wad debug disable category ssh	1885
diagnose wad debug disable category ssl	1885
diagnose wad debug disable category stream	1886
diagnose wad debug disable category svc_conn	1886
diagnose wad debug disable category sys	1886
diagnose wad debug disable category tls_fingerprint	1886
diagnose wad debug disable category tunnel	1886
diagnose wad debug disable category uih	1886
diagnose wad debug disable category video	1887
diagnose wad debug disable category vs	1887
diagnose wad debug disable category waf	1887
diagnose wad debug disable category webcache	1887
diagnose wad debug disable category ztna_portal	1887
diagnose wad debug display	1887
diagnose wad debug display pid	1888
diagnose wad debug display pid disable	1888
diagnose wad debug display pid enable	1888
diagnose wad debug enable	1888
diagnose wad debug enable all	1888
diagnose wad debug enable category	1888
diagnose wad debug enable category aio	1889
diagnose wad debug enable category all	1889
diagnose wad debug enable category antiphish	1889
diagnose wad debug enable category auth	1889
diagnose wad debug enable category autotest	1889
diagnose wad debug enable category bytecache	1889
diagnose wad debug enable category cache_server	1890
diagnose wad debug enable category casb	1890
diagnose wad debug enable category cifs	1890

diagnose wad debug enable category cmgr	1890
diagnose wad debug enable category config	1890
diagnose wad debug enable category csvc	1890
diagnose wad debug enable category detail	1891
diagnose wad debug enable category devuln	1891
diagnose wad debug enable category diag	1891
diagnose wad debug enable category dispatcher	1891
diagnose wad debug enable category dns	1891
diagnose wad debug enable category dskd	1891
diagnose wad debug enable category email	1892
diagnose wad debug enable category extension	1892
diagnose wad debug enable category ftp	1892
diagnose wad debug enable category http	1892
diagnose wad debug enable category http2	1892
diagnose wad debug enable category http3	1892
diagnose wad debug enable category icap	1893
diagnose wad debug enable category icap_server	1893
diagnose wad debug enable category icbsvc	1893
diagnose wad debug enable category info	1893
diagnose wad debug enable category ips	1893
diagnose wad debug enable category isolator	1893
diagnose wad debug enable category license	1894
diagnose wad debug enable category mapi	1894
diagnose wad debug enable category memblk	1894
diagnose wad debug enable category monitor	1894
diagnose wad debug enable category packet	1894
diagnose wad debug enable category policy	1894
diagnose wad debug enable category policy_test	1895
diagnose wad debug enable category proc	1895
diagnose wad debug enable category quic	1895
diagnose wad debug enable category quic_cc	1895
diagnose wad debug enable category rev_conn	1895
diagnose wad debug enable category rpc	1895
diagnose wad debug enable category scan	1896
diagnose wad debug enable category scp	1896
diagnose wad debug enable category session	1896
diagnose wad debug enable category sftp	1896
diagnose wad debug enable category socks	1896
diagnose wad debug enable category ssh	1896
diagnose wad debug enable category ssl	1897
diagnose wad debug enable category stream	1897
diagnose wad debug enable category svc_conn	1897
diagnose wad debug enable category sys	1897
diagnose wad debug enable category tls_fingerprint	1897
diagnose wad debug enable category tunnel	1897
diagnose wad debug enable category uih	1898
diagnose wad debug enable category video	1898
diagnose wad debug enable category vs	1898
diagnose wad debug enable category waf	1898

diagnose wad debug enable category webcache	1898
diagnose wad debug enable category ztna_portal	1898
diagnose wad debug enable level	1899
diagnose wad debug enable level error	1899
diagnose wad debug enable level info	1899
diagnose wad debug enable level verbose	1899
diagnose wad debug enable level warn	1899
diagnose wad debug ips-db	1900
diagnose wad debug ips-db status	1900
diagnose wad debug ips-filter	1900
diagnose wad debug ips-filter aid	1900
diagnose wad debug ips-filter all	1900
diagnose wad debug ips-filter clear	1900
diagnose wad debug ips-filter show	1901
diagnose wad debug ips-filter vid	1901
diagnose wad debug save-http-req-crash	1901
diagnose wad debug save-http-req-crash disable	1901
diagnose wad debug save-http-req-crash enable	1901
diagnose wad debug show	1901
diagnose wad dev	1902
diagnose wad dev fcnacd	1902
diagnose wad dev fcnacd delete	1902
diagnose wad dev fcnacd ip-err	1902
diagnose wad dev fcnacd uid-err	1902
diagnose wad dev fcnacd update	1902
diagnose wad dev query-by	1903
diagnose wad dev query-by ipv4	1903
diagnose wad dev query-by ipv6	1903
diagnose wad dev query-by uid	1903
diagnose wad dev-vuln	1903
diagnose wad dev-vuln query	1903
diagnose wad dev-vuln query-by-id	1904
diagnose wad dev-vuln query-ftgd	1904
diagnose wad dynamic-bypass	1904
diagnose wad dynamic-bypass clear	1904
diagnose wad dynamic-bypass flush	1904
diagnose wad dynamic-bypass show	1904
diagnose wad exp-fw-policy-test	1905
diagnose wad exp-fw-policy-test-save	1905
diagnose wad filter	1905
diagnose wad filter clear	1906
diagnose wad filter dport	1906
diagnose wad filter drop-unknown-session	1906
diagnose wad filter dst	1906
diagnose wad filter dst6	1906
diagnose wad filter explicit-policy	1907
diagnose wad filter firewall-policy	1907
diagnose wad filter list	1907
diagnose wad filter negate	1907

diagnose wad filter process-id	1908
diagnose wad filter process-id-by-src	1908
diagnose wad filter process-type	1908
diagnose wad filter protocol	1908
diagnose wad filter proxy-policy-list-increment	1909
diagnose wad filter sport	1909
diagnose wad filter src	1909
diagnose wad filter src6	1910
diagnose wad filter vd	1910
diagnose wad fw-policy-test-get	1910
diagnose wad health	1910
diagnose wad health debug	1910
diagnose wad health fs	1911
diagnose wad health worker	1911
diagnose wad history	1911
diagnose wad history clear	1911
diagnose wad history list	1911
diagnose wad icap	1912
diagnose wad icap list	1912
diagnose wad kxp	1912
diagnose wad kxp clear	1912
diagnose wad kxp list	1912
diagnose wad license	1912
diagnose wad license clear	1913
diagnose wad license debug	1913
diagnose wad license debug fcas	1913
diagnose wad license debug fnbi	1913
diagnose wad license debug furl	1913
diagnose wad license detail	1914
diagnose wad license glob-usage	1914
diagnose wad license glob-usage 15seconds	1914
diagnose wad license glob-usage 5minutes	1914
diagnose wad license glob-usage days	1914
diagnose wad license glob-usage hours	1914
diagnose wad license glob-usage months	1915
diagnose wad license glob-usage weeks	1915
diagnose wad license glob-usage years	1915
diagnose wad license summary	1915
diagnose wad license test	1915
diagnose wad license usage	1915
diagnose wad license usage 15seconds	1916
diagnose wad license usage 5minutes	1916
diagnose wad license usage days	1916
diagnose wad license usage hours	1916
diagnose wad license usage months	1916
diagnose wad license usage weeks	1916
diagnose wad license usage years	1917
diagnose wad memory	1917
diagnose wad memory monitor	1917

diagnose wad memory monitor disable	1917
diagnose wad memory monitor enable	1917
diagnose wad memory monitor interval	1917
diagnose wad memory monitor list	1918
diagnose wad memory monitor max-report-files	1918
diagnose wad memory monitor mem-threshold-red	1918
diagnose wad memory overused	1918
diagnose wad memory report	1918
diagnose wad memory sum	1919
diagnose wad memory track	1919
diagnose wad memory workers	1919
diagnose wad nbi	1919
diagnose wad nbi license	1919
diagnose wad nbi packages	1920
diagnose wad nbi status	1920
diagnose wad process	1920
diagnose wad process YouTube-filter-cache-service	1920
diagnose wad process algo	1920
diagnose wad process byte-cache	1921
diagnose wad process cache-service-cs	1921
diagnose wad process cache-service-db	1921
diagnose wad process cert-inspection	1922
diagnose wad process cert-manager	1922
diagnose wad process config-notify	1922
diagnose wad process debug	1923
diagnose wad process dev-vuln	1923
diagnose wad process dispatcher	1923
diagnose wad process ia-cache	1924
diagnose wad process informer	1924
diagnose wad process isolator	1924
diagnose wad process manager	1925
diagnose wad process object-cache	1925
diagnose wad process preload daemon	1925
diagnose wad process reverse-connector	1926
diagnose wad process staled-worker	1926
diagnose wad process tls-fgpt-service	1926
diagnose wad process traffic aggregator	1927
diagnose wad process unknown	1927
diagnose wad process user-info	1927
diagnose wad process user-info-history	1928
diagnose wad process worker	1928
diagnose wad report	1928
diagnose wad report policy	1928
diagnose wad report session	1929
diagnose wad report user	1929
diagnose wad restore	1929
diagnose wad restore cdn-rules	1929
diagnose wad restore cdn-rules all	1929
diagnose wad session	1929

diagnose wad session clear	1930
diagnose wad session list	1930
diagnose wad session list-http2	1930
diagnose wad sshproxy	1930
diagnose wad sshproxy clear	1930
diagnose wad sshproxy list	1930
diagnose wad stats	1931
diagnose wad stats algo	1931
diagnose wad stats algo.antiphish	1931
diagnose wad stats algo.casb	1931
diagnose wad stats algo.dev_info	1932
diagnose wad stats algo.dev_type	1932
diagnose wad stats algo.fast_tb	1932
diagnose wad stats algo.fw_policy	1932
diagnose wad stats algo.icap_client	1932
diagnose wad stats algo.ips	1933
diagnose wad stats algo.ips_builder	1933
diagnose wad stats algo.krl	1933
diagnose wad stats algo.proc_common	1933
diagnose wad stats algo.sec_prof	1934
diagnose wad stats algo.ssl	1934
diagnose wad stats algo.url_filter	1934
diagnose wad stats algo.urlredirect	1934
diagnose wad stats cache_service	1935
diagnose wad stats cache_service.proc_common	1935
diagnose wad stats cache_service.tcp	1935
diagnose wad stats cic	1935
diagnose wad stats cic.proc_common	1935
diagnose wad stats cmgr	1936
diagnose wad stats cmgr.cert_cache	1936
diagnose wad stats cmgr.cert_service	1936
diagnose wad stats cmgr.dns_req	1936
diagnose wad stats cmgr.http_engine	1937
diagnose wad stats cmgr.proc_common	1937
diagnose wad stats cmgr.quic	1937
diagnose wad stats cmgr.ssl	1937
diagnose wad stats cmgr.tcp	1938
diagnose wad stats common	1938
diagnose wad stats common.dc_ad_dns	1938
diagnose wad stats common.diag	1938
diagnose wad stats common.sched	1938
diagnose wad stats common.ses_stats	1939
diagnose wad stats common.waps	1939
diagnose wad stats config	1939
diagnose wad stats config.proc_common	1939
diagnose wad stats config.shm_stats	1940
diagnose wad stats config.stream_scan	1940
diagnose wad stats debug	1940
diagnose wad stats debug.crash_handler	1940

diagnose wad stats debug.proc_common	1941
diagnose wad stats dev_vuln	1941
diagnose wad stats dev_vuln.dns_req	1941
diagnose wad stats dev_vuln.proc_common	1941
diagnose wad stats dev_vuln.ssl	1941
diagnose wad stats dev_vuln.tcp	1942
diagnose wad stats dispatcher	1942
diagnose wad stats dispatcher.cifs	1942
diagnose wad stats dispatcher.dns_proxy	1942
diagnose wad stats dispatcher.icap_local_server	1943
diagnose wad stats dispatcher.proc_common	1943
diagnose wad stats dispatcher.ssh	1943
diagnose wad stats dispatcher.tcp	1943
diagnose wad stats dispatcher.tunnel	1944
diagnose wad stats fgpt	1944
diagnose wad stats fgpt.proc_common	1944
diagnose wad stats ia_cache	1944
diagnose wad stats ia_cache.proc_common	1944
diagnose wad stats informer	1945
diagnose wad stats informer.dev_info	1945
diagnose wad stats informer.dev_type	1945
diagnose wad stats informer.proc_common	1945
diagnose wad stats informer.ztna_jwt	1946
diagnose wad stats isolator	1946
diagnose wad stats isolator.dns_req	1946
diagnose wad stats isolator.proc_common	1946
diagnose wad stats isolator.ssl	1947
diagnose wad stats isolator.tcp	1947
diagnose wad stats mgr	1947
diagnose wad stats mgr.proc_common	1947
diagnose wad stats mgr.shm_stats	1947
diagnose wad stats uih	1948
diagnose wad stats uih.proc_common	1948
diagnose wad stats usr_info	1948
diagnose wad stats usr_info.dev_info	1948
diagnose wad stats usr_info.dev_type	1949
diagnose wad stats usr_info.dns_req	1949
diagnose wad stats usr_info.proc_common	1949
diagnose wad stats usr_info.ssl	1949
diagnose wad stats usr_info.tcp	1950
diagnose wad stats vfcs	1950
diagnose wad stats vfcs.proc_common	1950
diagnose wad stats worker	1950
diagnose wad stats worker.aio	1950
diagnose wad stats worker.antiphish	1951
diagnose wad stats worker.app_mgr	1951
diagnose wad stats worker.auth	1951
diagnose wad stats worker.casb	1951
diagnose wad stats worker.cert_cache	1952

diagnose wad stats worker.cifs	1952
diagnose wad stats worker.config_delta	1952
diagnose wad stats worker.conn_pool	1952
diagnose wad stats worker.dev_info	1953
diagnose wad stats worker.dev_type	1953
diagnose wad stats worker.dns_proxy	1953
diagnose wad stats worker.dns_req	1953
diagnose wad stats worker.fast_match	1953
diagnose wad stats worker.fw_policy	1954
diagnose wad stats worker.hauth_uid_cache	1954
diagnose wad stats worker.http_engine	1954
diagnose wad stats worker.http_ffbk	1954
diagnose wad stats worker.http_scan	1955
diagnose wad stats worker.http_srv_selector	1955
diagnose wad stats worker.http_view	1955
diagnose wad stats worker.icap_client	1955
diagnose wad stats worker.icap_local_server	1956
diagnose wad stats worker.icap_parser	1956
diagnose wad stats worker.icap_remote_server	1956
diagnose wad stats worker.infection_cache	1956
diagnose wad stats worker.ipseng	1956
diagnose wad stats worker.krl	1957
diagnose wad stats worker.pol_test	1957
diagnose wad stats worker.policy_profile	1957
diagnose wad stats worker.proc_common	1957
diagnose wad stats worker.protos	1958
diagnose wad stats worker.quic	1958
diagnose wad stats worker.scan_cache	1958
diagnose wad stats worker.sec_prof	1958
diagnose wad stats worker.shm_stats	1959
diagnose wad stats worker.ssh	1959
diagnose wad stats worker.ssl	1959
diagnose wad stats worker.sysmem	1959
diagnose wad stats worker.tcp	1959
diagnose wad stats worker.traffic_mirror	1960
diagnose wad stats worker.tunnel	1960
diagnose wad stats worker.url_filter	1960
diagnose wad stats worker.url_match	1960
diagnose wad stats worker.urlredir	1961
diagnose wad stats worker.vs_cert_cache	1961
diagnose wad stats worker.ztna_jwt	1961
diagnose wad stream-scan	1961
diagnose wad stream-scan av-intf	1962
diagnose wad stream-scan av-intf disable	1962
diagnose wad stream-scan av-intf enable	1962
diagnose wad stream-scan av-test	1962
diagnose wad tcp-connection	1962
diagnose wad tcp-connection list	1962
diagnose wad toggle	1963

diagnose wad tp-fw-policy-test	1963
diagnose wad tp-fw-policy-test-save	1963
diagnose wad tunnel	1964
diagnose wad tunnel clear	1964
diagnose wad tunnel list	1964
diagnose wad uih	1964
diagnose wad uih chart	1965
diagnose wad uih chart range	1965
diagnose wad uih chart summary	1965
diagnose wad url-lookup	1965
diagnose wad user	1965
diagnose wad user clear	1965
diagnose wad user count	1966
diagnose wad user device	1966
diagnose wad user domain-controller	1966
diagnose wad user domain-controller dns	1966
diagnose wad user domain-controller dns list	1966
diagnose wad user domain-controller dns test	1967
diagnose wad user exchange	1967
diagnose wad user exchange get-matches	1967
diagnose wad user exchange query-rows	1967
diagnose wad user exchange reset	1967
diagnose wad user exchange resolve-names	1967
diagnose wad user exchange test-auto-discover	1968
diagnose wad user list	1968
diagnose wad webcache	1968
diagnose wad webcache clear	1968
diagnose wad webcache list	1968
diagnose wad webproxy	1969
diagnose wad webproxy clear	1969
diagnose wad webproxy forward-server	1969
diagnose wad webproxy forward-server detail	1969
diagnose wad webproxy forward-server summary	1969
diagnose wad webproxy forward-server-group	1969
diagnose wad webproxy list	1970
diagnose wad worker	1970
diagnose wad worker async-ut	1970
diagnose wad worker avscan	1970
diagnose wad worker avscan clear	1970
diagnose wad worker avscan list	1970
diagnose wad worker bytecache	1971
diagnose wad worker bytecache clear	1971
diagnose wad worker bytecache flush	1971
diagnose wad worker bytecache stats	1971
diagnose wad worker bytecache toggle	1971
diagnose wad worker bytecache toggle all	1972
diagnose wad worker bytecache toggle config	1972
diagnose wad worker bytecache toggle create	1972
diagnose wad worker bytecache toggle read	1972

diagnose wad worker cookie	1972
diagnose wad worker cookie map	1973
diagnose wad worker filter	1973
diagnose wad worker filter clear	1973
diagnose wad worker filter list	1973
diagnose wad worker imagecache	1973
diagnose wad worker imagecache flush	1973
diagnose wad worker imagecache stats	1974
diagnose wad worker memcache	1974
diagnose wad worker memcache clear	1974
diagnose wad worker memcache flush	1974
diagnose wad worker memcache stats	1974
diagnose wad worker memcache toggle	1975
diagnose wad worker memcache toggle all	1975
diagnose wad worker memcache toggle config	1975
diagnose wad worker memcache toggle create	1975
diagnose wad worker memcache toggle read	1975
diagnose wad worker oidc	1976
diagnose wad worker oidc clear-jwks	1976
diagnose wad worker oidc refresh-server	1976
diagnose wad worker oidc servers	1976
diagnose wad worker oidc sessions	1977
diagnose wad worker peer	1977
diagnose wad worker peer clear	1977
diagnose wad worker peer list	1977
diagnose wad worker policy	1977
diagnose wad worker policy clear	1977
diagnose wad worker policy list	1978
diagnose wad worker restart	1978
diagnose wad worker saml	1978
diagnose wad worker scripts	1978
diagnose wad worker scripts clear	1978
diagnose wad worker scripts list	1979
diagnose wad worker webcache	1979
diagnose wad worker webcache clear	1979
diagnose wad worker webcache flush	1979
diagnose wad worker webcache stats	1979
diagnose wad worker webcache summary	1980
diagnose wad worker webcache toggle	1980
diagnose wad worker webcache toggle abort	1980
diagnose wad worker webcache toggle add_ref	1980
diagnose wad worker webcache toggle all	1980
diagnose wad worker webcache toggle append	1981
diagnose wad worker webcache toggle config	1981
diagnose wad worker webcache toggle create	1981
diagnose wad worker webcache toggle read	1981
diagnose wad worker webcache toggle remove	1981
diagnose wad worker webcache toggle resolve	1982
diagnose wad worker webcache toggle update	1982

diagnose wadbd	1982
diagnose wadbd clear	1982
diagnose wadbd log-show	1983
diagnose wadbd restart	1983
diagnose wadbd stats	1983
diagnose waf	1983
diagnose waf dump	1983
diagnose waf info	1984
diagnose webfilter	1984
diagnose webfilter bword	1984
diagnose webfilter bword matchfilter	1984
diagnose webfilter fortiguard	1985
diagnose webfilter fortiguard cache	1985
diagnose webfilter fortiguard cache dump	1985
diagnose webfilter fortiguard cache obs	1985
diagnose webfilter fortiguard cache prefix	1985
diagnose webfilter fortiguard cache tree	1986
diagnose webfilter fortiguard cache ttl	1986
diagnose webfilter fortiguard override	1986
diagnose webfilter fortiguard override all-admin-override	1986
diagnose webfilter fortiguard override all-user-override	1986
diagnose webfilter fortiguard override all-warning	1986
diagnose webfilter fortiguard override obs	1987
diagnose webfilter fortiguard override statistics	1987
diagnose webfilter fortiguard statistics	1987
diagnose webfilter fortiguard statistics flush	1987
diagnose webfilter fortiguard statistics list	1987
diagnose web-ui	1987
diagnose web-ui api-cache	1988
diagnose web-ui api-cache statistic	1988
diagnose web-ui api-stats	1988
diagnose web-ui api-stats disable	1989
diagnose web-ui api-stats enable	1989
diagnose web-ui api-stats list	1989
diagnose web-ui api-stats reset	1989
diagnose web-ui api-stats status	1989
diagnose web-ui backtrace	1989
diagnose web-ui backtrace clear	1990
diagnose web-ui backtrace disable	1990
diagnose web-ui backtrace enable	1990
diagnose web-ui backtrace httpsd	1990
diagnose web-ui backtrace status	1990
diagnose web-ui cache	1990
diagnose web-ui cache disable	1991
diagnose web-ui cache enable	1991
diagnose web-ui localization	1991
diagnose web-ui localization disable	1991
diagnose web-ui localization enable	1991
diagnose web-ui next-gen-table	1991

diagnose web-ui next-gen-table disable	1992
diagnose web-ui next-gen-table enable	1992
CLI execute commands	1993
execute api-user	1995
execute api-user generate-key	1995
execute auto-script	1996
execute auto-script backup ftp	1996
execute auto-script backup tftp	1996
execute auto-script delete	1997
execute auto-script result	1997
execute auto-script start	1997
execute auto-script status	1997
execute auto-script stop	1998
execute auto-script stopall	1998
execute backup	1998
execute backup config flash	1999
execute backup config ftp	1999
execute backup config management-station	2000
execute backup config sftp	2000
execute backup config tftp	2000
execute backup config usb	2001
execute backup config usb-mode	2001
execute backup disk alllogs ftp	2001
execute backup disk alllogs tftp	2002
execute backup disk alllogs usb	2002
execute backup disk ipsarchives ftp	2002
execute backup disk ipsarchives tftp	2002
execute backup disk ipsarchives usb	2003
execute backup disk log ftp	2003
execute backup disk log tftp	2003
execute backup disk log usb	2004
execute backup full-config ftp	2004
execute backup full-config sftp	2004
execute backup full-config tftp	2005
execute backup full-config usb	2005
execute backup full-config usb-mode	2005
execute backup ipsuserdefsig ftp	2006
execute backup ipsuserdefsig tftp	2006
execute backup memory alllogs ftp	2006
execute backup memory alllogs tftp	2006
execute backup memory log ftp	2007
execute backup memory log tftp	2007
execute backup obfuscated-config ftp	2007
execute backup obfuscated-config management-station	2008
execute backup obfuscated-config sftp	2008
execute backup obfuscated-config tftp	2009
execute backup obfuscated-config usb	2009
execute backup obfuscated-full-config ftp	2009
execute backup obfuscated-full-config sftp	2010

execute backup obfuscated-full-config tftp	2010
execute backup obfuscated-full-config usb	2010
execute backup obfuscated-yaml-config ftp	2011
execute backup obfuscated-yaml-config tftp	2011
execute backup tls-finger-print tftp	2011
execute backup yaml-config ftp	2012
execute backup yaml-config tftp	2012
execute batch	2012
execute batch end	2013
execute batch lastlog	2013
execute batch start	2013
execute batch status	2013
execute central-mgmt	2013
execute central-mgmt register-device	2013
execute central-mgmt set-mgmt-id	2014
execute central-mgmt unregister-device	2014
execute cfg	2014
execute cfg reload	2014
execute cfg save	2015
execute clear	2015
execute clear system arp table	2015
execute cli	2015
execute cli check-template-status	2015
execute cli status-msg-only	2016
execute cloud-service	2016
execute cloud-service gen-jwt-as-token	2016
execute cloud-service list	2016
execute cloud-service manual-gen-jwt-as-token	2017
execute config-transaction	2017
execute config-transaction abort	2017
execute config-transaction commit	2017
execute config-transaction start	2017
execute cpu	2018
execute cpu add	2018
execute cpu show	2018
execute date	2018
execute device-upgrade	2019
execute device-upgrade cancel	2019
execute device-upgrade immediate	2019
execute dhcp	2019
execute dhcp lease-clear	2020
execute dhcp lease-list	2020
execute dhcp6	2020
execute dhcp6 lease-clear	2021
execute dhcp6 lease-list	2021
execute disconnect-admin-session	2021
execute disk	2021
execute disk format	2022

execute disk list	2022
execute disk scan	2022
execute enter	2022
execute erase-disk	2022
execute fabric-vpn	2023
execute fabric-vpn flush-setup	2023
execute fabric-vpn update-setup	2023
execute factoryreset	2023
execute factoryreset2	2023
execute factoryreset-for-central-management	2024
execute factoryreset-shutdown	2024
execute fctems	2024
execute fctems is-verified	2025
execute fctems unverify	2025
execute fctems verify	2025
execute federated-upgrade	2025
execute federated-upgrade cancel	2026
execute federated-upgrade initialize	2026
execute federated-upgrade quick-fortigate-upgrade	2026
execute federated-upgrade quick-full-upgrade	2026
execute federated-upgrade restart	2027
execute federated-upgrade safe-cancel	2027
execute federated-upgrade status	2027
execute fips	2027
execute fips tftp-drbg-entropy-source	2028
execute fips tftp-test-vectors	2028
execute firewall	2028
execute firewall ssh generate local-ca	2028
execute firewall ssh generate local-key	2029
execute formatlogdisk	2029
execute forticloud-sandbox	2029
execute forticloud-sandbox region	2029
execute forticloud-sandbox update	2029
execute fortiguard-log	2030
execute fortiguard-log certificate-activation	2030
execute fortiguard-log migration	2030
execute fortiguard-log update	2030
execute fortiguard-message	2031
execute fortiguard-message add	2031
execute fortiguard-message info	2031
execute fortiguard-message update	2031
execute fortimanager	2031
execute fortimanager fetch	2032
execute fortimanager register	2032
execute fortitoken	2032
execute fortitoken activate	2032
execute fortitoken import ftp	2033

execute fortitoken import tftp	2033
execute fortitoken import usb	2033
execute fortitoken import-sn-file	2033
execute fortitoken sync	2034
execute fortitoken-cloud	2034
execute fortitoken-cloud migrate-ftm	2034
execute fortitoken-cloud new	2035
execute fortitoken-cloud show	2035
execute fortitoken-cloud sync	2035
execute fortitoken-cloud trial	2035
execute fortitoken-cloud update	2035
execute fortitoken-mobile	2036
execute fortitoken-mobile import	2036
execute fortitoken-mobile poll	2036
execute fortitoken-mobile provision	2036
execute fortitoken-mobile renew	2036
execute fsso	2037
execute fsso refresh	2037
execute ha	2037
execute ha disconnect	2037
execute ha failover set	2038
execute ha failover status	2038
execute ha failover unset	2038
execute ha manage	2038
execute ha synchronize	2039
execute http-view	2039
execute http-view report	2039
execute interface	2039
execute interface dhcp6client-renew	2040
execute interface dhcpclient-renew	2040
execute interface pppoe-reconnect	2040
execute internet-service4	2040
execute internet-service4 refresh	2041
execute internet-service6	2041
execute internet-service6 refresh	2041
execute ipam	2041
execute ipam create-dhcp-server	2041
execute kmip	2042
execute kmip create	2042
execute kmip destroy	2042
execute kmip get	2043
execute kmip locate	2043
execute kmip rekey	2043
execute log	2043
execute log backup ftp	2044
execute log backup local	2045
execute log backup tftp	2045
execute log delete	2045

execute log delete-all	2045
execute log detail	2046
execute log display	2046
execute log filter category	2046
execute log filter device	2046
execute log filter dump	2046
execute log filter field	2047
execute log filter free-style	2047
execute log filter ha-member	2047
execute log filter local-search-mode	2048
execute log filter max-checklines	2048
execute log filter pre-fetch-pages	2048
execute log filter reset	2048
execute log filter start-line	2049
execute log filter view-lines	2049
execute log flush-cache	2049
execute log flush-cache-all	2049
execute log fortianalyzer manual-failover	2049
execute log fortianalyzer test-connectivity	2050
execute log fortianalyzer-cloud test-connectivity	2050
execute log fortianalyzer2 manual-failover	2050
execute log fortianalyzer3 manual-failover	2050
execute log fortiguard test-connectivity	2050
execute log list	2050
execute log raw-backup ftp	2051
execute log raw-backup tftp	2051
execute log restore	2051
execute log roll	2051
execute log shift-time	2052
execute log upload	2052
execute log upload-progress	2052
execute mem	2052
execute mem add	2052
execute nethsm	2053
execute nethsm primus clear-pkcs-provider-log	2053
execute nethsm primus clear-primus-log	2054
execute nethsm primus delete-object	2054
execute nethsm primus dump-pkcs-provider-log	2054
execute nethsm primus dump-primus-log	2054
execute nethsm primus inspect-primus-library-info	2054
execute nethsm primus list-objects	2054
execute nethsm primus upload-primus-cfg	2055
execute nethsm primus upload-primus-cfg-raw	2055
execute nethsm safenet clear-log	2055
execute nethsm safenet client-cert-create	2055
execute nethsm safenet client-cert-export ftp	2055
execute nethsm safenet client-cert-export tftp	2056
execute nethsm safenet client-cert-show	2056
execute nethsm safenet config-export ftp	2056

execute nethsm safenet config-export tftp	2057
execute nethsm safenet config-import ftp	2057
execute nethsm safenet config-import tftp	2057
execute nethsm safenet config-show	2057
execute nethsm safenet diagnose	2058
execute nethsm safenet hagroup-add	2058
execute nethsm safenet hagroup-del	2058
execute nethsm safenet hagroup-list	2058
execute nethsm safenet register	2058
execute nethsm safenet reset	2059
execute nethsm safenet restore-conf	2059
execute nethsm safenet set-conf-opt	2059
execute nethsm safenet show-log	2059
execute nethsm safenet status	2059
execute nethsm safenet unregister	2060
execute nsx	2060
execute nsx group delete	2060
execute nsx group import	2060
execute nsx group list	2061
execute ping	2061
execute ping6	2061
execute ping6-options	2061
execute ping6-options adaptive-ping	2062
execute ping6-options data-size	2062
execute ping6-options interface	2062
execute ping6-options interval	2062
execute ping6-options pattern	2063
execute ping6-options repeat-count	2063
execute ping6-options reset	2063
execute ping6-options source6	2063
execute ping6-options timeout	2064
execute ping6-options tos	2064
execute ping6-options ttl	2064
execute ping6-options validate-reply	2064
execute ping6-options view-settings	2064
execute ping-options	2065
execute ping-options adaptive-ping	2065
execute ping-options data-size	2065
execute ping-options df-bit	2066
execute ping-options interface	2066
execute ping-options interval	2066
execute ping-options pattern	2066
execute ping-options repeat-count	2067
execute ping-options reset	2067
execute ping-options source	2067
execute ping-options timeout	2067
execute ping-options tos	2067
execute ping-options ttl	2068
execute ping-options use-sdwan	2068

execute ping-options validate-reply	2068
execute ping-options view-settings	2068
execute policy-packet-capture	2069
execute policy-packet-capture delete-all	2069
execute preload	2069
execute preload http-transaction-log disable	2069
execute preload http-transaction-log enable	2069
execute preload list	2070
execute preload show-log	2070
execute preload url	2070
execute preload url-delete	2070
execute private-encryption-key	2071
execute private-encryption-key sample	2071
execute private-encryption-key verify	2071
execute reboot	2071
execute report	2072
execute report flush-cache	2072
execute report recreate-db	2072
execute report run	2072
execute report sandbox-status	2072
execute report-config	2073
execute report-config reset	2073
execute restore	2073
execute restore av ftp	2074
execute restore av tftp	2074
execute restore config dhcp	2075
execute restore config flash	2075
execute restore config ftp	2075
execute restore config management-station normal	2076
execute restore config management-station script	2076
execute restore config management-station template	2076
execute restore config tftp	2076
execute restore config usb	2077
execute restore config usb-mode	2077
execute restore image flash	2077
execute restore image ftp	2077
execute restore image management-station	2078
execute restore image tftp	2078
execute restore image url	2078
execute restore image usb	2079
execute restore ips ftp	2079
execute restore ips tftp	2079
execute restore ipsuserdefsig ftp	2079
execute restore ipsuserdefsig tftp	2080
execute restore manual-license ftp	2080
execute restore manual-license tftp	2080
execute restore other-objects ftp	2081
execute restore other-objects tftp	2081

execute restore script ftp	2081
execute restore script lastlog	2082
execute restore script scp	2082
execute restore script tftp	2082
execute restore vmlicense ftp	2083
execute restore vmlicense tftp	2083
execute revision	2083
execute revision delete config	2083
execute revision delete image	2084
execute revision list config	2084
execute revision list image	2084
execute send-fds-statistics	2084
execute send-fmg-list	2085
execute set	2085
execute set system session filter clear all	2086
execute set system session filter clear dport	2086
execute set system session filter clear dst	2086
execute set system session filter clear duration	2086
execute set system session filter clear expire	2086
execute set system session filter clear policy	2086
execute set system session filter clear proto	2087
execute set system session filter clear sport	2087
execute set system session filter clear src	2087
execute set system session filter clear vd	2087
execute set system session filter dport	2087
execute set system session filter dst	2087
execute set system session filter duration	2088
execute set system session filter expire	2088
execute set system session filter list	2088
execute set system session filter negate dport	2088
execute set system session filter negate dst	2088
execute set system session filter negate duration	2089
execute set system session filter negate expire	2089
execute set system session filter negate policy	2089
execute set system session filter negate proto	2089
execute set system session filter negate sport	2089
execute set system session filter negate src	2089
execute set system session filter negate vd	2090
execute set system session filter policy	2090
execute set system session filter proto	2090
execute set system session filter sport	2090
execute set system session filter src	2090
execute set system session filter vd	2091
execute shutdown	2091
execute speed-test	2091
execute speed-test-custom	2092
execute speed-test-ipsec	2092
execute speed-test-options	2092

execute speed-test-options blksize	2093
execute speed-test-options burst	2093
execute speed-test-options ctrl-port	2093
execute speed-test-options duration	2093
execute speed-test-options get-token	2094
execute speed-test-options max-down	2094
execute speed-test-options max-up	2094
execute speed-test-options protocol	2094
execute speed-test-options reset	2095
execute speed-test-options reset-token	2095
execute speed-test-options server-port	2095
execute speed-test-options set-shaper	2095
execute speed-test-options show	2095
execute speed-test-options tos	2096
execute speed-test-server	2096
execute speed-test-server download	2096
execute speed-test-server list	2096
execute ssh	2096
execute ssh6	2097
execute ssh6-options	2097
execute ssh6-options interface	2097
execute ssh6-options reset	2097
execute ssh6-options source6	2098
execute ssh6-options view-settings	2098
execute ssh-options	2098
execute ssh-options interface	2098
execute ssh-options reset	2099
execute ssh-options source	2099
execute ssh-options view-settings	2099
execute ssh-regen-keys	2099
execute sync-IPSec	2099
execute sync-session	2100
execute system	2100
execute system custom-language import	2100
execute system fortisandbox test-alternative-connectivity	2100
execute system fortisandbox test-primary-connectivity	2100
execute tac	2101
execute tac report	2101
execute telnet	2101
execute telnet-options	2101
execute telnet-options interface	2102
execute telnet-options reset	2102
execute telnet-options source	2102
execute telnet-options view-settings	2102
execute test	2102
execute test tftp-analytics-report	2103
execute time	2103

execute traceroute	2103
execute traceroute-options	2103
execute traceroute-options device	2104
execute traceroute-options queries	2104
execute traceroute-options reset	2104
execute traceroute-options source	2104
execute traceroute-options use-sdwan	2105
execute traceroute-options view-settings	2105
execute tracert6	2105
execute update-av	2105
execute update-external-resource	2105
execute update-ffdb-on-demand	2106
execute update-geo-ip	2106
execute update-ips	2106
execute update-list	2106
execute update-now	2106
execute update-src-vis	2107
execute upd-vd-license	2107
execute upload	2107
execute upload config ftp	2107
execute upload config tftp	2108
execute upload config usb	2108
execute upload fortinbi-installer cloud	2108
execute upload fortinbi-installer tftp	2109
execute upload fortinbi-isolator-image cloud	2109
execute upload fortinbi-isolator-image tftp	2109
execute upload image ftp	2109
execute upload image tftp	2110
execute upload image usb	2110
execute upload report-img ftp	2110
execute upload report-img tftp	2111
execute usb-device	2111
execute usb-device disconnect	2111
execute usb-device list	2111
execute usb-device modeswitch	2112
execute usb-disk	2112
execute usb-disk delete	2112
execute usb-disk eject	2112
execute usb-disk format	2113
execute usb-disk list	2113
execute usb-disk rename	2113
execute vm-license	2113
execute vm-license-options	2113
execute vm-license-options account-id	2114
execute vm-license-options account-password	2114
execute vm-license-options count	2114
execute vm-license-options government	2115

execute vm-license-options interval	2115
execute vm-license-options proxy	2115
execute vm-license-options reset	2115
execute vm-license-options show	2115
execute vm-license-options token	2116
execute vpn	2116
execute vpn certificate ca export tftp	2117
execute vpn certificate ca import auto	2117
execute vpn certificate ca import bundle	2117
execute vpn certificate ca import est	2117
execute vpn certificate ca import tftp	2118
execute vpn certificate crt import auto	2118
execute vpn certificate ems_ca import tftp	2118
execute vpn certificate hsm primus generate ec	2118
execute vpn certificate hsm primus generate rsa	2119
execute vpn certificate hsm primus load-key	2119
execute vpn certificate hsm safenet generate rsa	2119
execute vpn certificate hsm-local gch-get-versions	2119
execute vpn certificate hsm-local status	2120
execute vpn certificate hsm-local verify	2120
execute vpn certificate local export tftp	2120
execute vpn certificate local generate cmp-ec	2120
execute vpn certificate local generate cmp-rsa	2120
execute vpn certificate local generate default-gui-mgmt-cert	2121
execute vpn certificate local generate default-ssl-ca	2121
execute vpn certificate local generate default-ssl-ca-untrusted	2121
execute vpn certificate local generate default-ssl-key-certs	2121
execute vpn certificate local generate default-ssl-serv-key	2122
execute vpn certificate local generate ec	2122
execute vpn certificate local generate est	2122
execute vpn certificate local generate rsa	2122
execute vpn certificate local import tftp	2123
execute vpn certificate local verify	2123
execute vpn certificate remote export tftp	2123
execute vpn certificate remote import tftp	2123
execute vpn ipsec tunnel down	2124
execute vpn ipsec tunnel up	2124
execute wake-on-lan	2124
execute webcache	2125
execute webcache delete regular-expression	2125
execute webcache delete simple-string	2125
execute webcache delete status	2125
execute webcache delete wildcard	2126
execute webfilter	2126
execute webfilter quota-reset	2126

Change log

Date	Change Description
2025-04-09	Initial release.
2024-04-29	Updated config system interface on page 972.
2025-05-07	Updated config vpn ipsec phase1-interface on page 1285.

FortiProxy CLI Interface

This document describes FortiProxy 7.6.3 CLI commands that are used to configure and manage FortiProxy from the command line interface (CLI). For information on using the CLI, see the [FortiProxy 7.6.3 Administration Guide](#).

CLI configuration commands

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

The CLI syntax is created by processing the schema from FortiProxy models running FortiProxy 7.6.3 and reformatting the resultant CLI output. If you have comments on this content, its format, or requests for commands that are not included, contact us at techdoc@fortinet.com.

alertemail

This section includes syntax for the following commands:

- [config alertemail setting on page 75](#)

config alertemail setting

Configure alert email settings.

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

```

set severity [emergency|alert|...]
end

```

config alertemail setting

Parameter	Description	Type	Size	Default						
username	Name that appears in the From: field of alert emails (max. 63 characters).	string	Maximum length: 63							
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							
mailto3	Optional third email address to send alert email to (max. 63 characters).	string	Maximum length: 63							
filter-mode	How to filter log messages that are sent to alert emails.	option	-	category						
	<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.									
email-interval	Interval between sending alert emails (1 - 99999 min, default = 5).	integer	Minimum value: 1 Maximum value: 99999	5						
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS logs in alert email.</td></tr><tr><td>disable</td><td>Disable IPS logs in alert email.</td></tr></table>				Option	Description	enable	Enable IPS logs in alert email.	disable	Disable IPS logs in alert email.
Option	Description									
enable	Enable IPS logs in alert email.									
disable	Disable IPS logs in alert email.									
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.									

Parameter	Description	Type	Size	Default						
HA-logs	Enable/disable HA logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable HA logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable HA logs in alert email.	<i>disable</i>	Disable HA logs in alert email.			
Option	Description									
<i>enable</i>	Enable HA logs in alert email.									
<i>disable</i>	Disable HA logs in alert email.									
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec error logs in alert email.	<i>disable</i>	Disable IPsec error logs in alert email.			
Option	Description									
<i>enable</i>	Enable IPsec error logs in alert email.									
<i>disable</i>	Disable IPsec error logs 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><i>enable</i></td><td>Enable FortiGuard update logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard update logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard update logs in alert email.	<i>disable</i>	Disable FortiGuard update logs in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard update logs in alert email.									
<i>disable</i>	Disable FortiGuard update logs in alert email.									
PPP-errors-logs	Enable/disable PPP error logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PPP error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable PPP error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable PPP error logs in alert email.	<i>disable</i>	Disable PPP error logs in alert email.			
Option	Description									
<i>enable</i>	Enable PPP error logs in alert email.									
<i>disable</i>	Disable PPP error logs in alert email.									
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-	disable						
	<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.									
webfilter-logs	Enable/disable web filter logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable web filter logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable web filter logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable web filter logs in alert email.	<i>disable</i>	Disable web filter logs in alert email.			
Option	Description									
<i>enable</i>	Enable web filter logs in alert email.									
<i>disable</i>	Disable web filter logs in alert email.									

Parameter	Description	Type	Size	Default						
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.									
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable violation traffic logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable violation traffic logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable violation traffic logs in alert email.	<i>disable</i>	Disable violation traffic logs in alert email.			
Option	Description									
<i>enable</i>	Enable violation traffic logs in alert email.									
<i>disable</i>	Disable violation traffic logs in alert email.									
admin-login-logs	Enable/disable administrator login/logout logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable administrator login/logout logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable administrator login/logout logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable administrator login/logout logs in alert email.	<i>disable</i>	Disable administrator login/logout logs in alert email.			
Option	Description									
<i>enable</i>	Enable administrator login/logout logs in alert email.									
<i>disable</i>	Disable administrator login/logout logs in alert email.									
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><i>enable</i></td><td>Enable FortiGuard license expiration warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard license expiration warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.	<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.									
<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.									
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><i>enable</i></td><td>Enable disk usage warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable disk usage warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable disk usage warnings in alert email.	<i>disable</i>	Disable disk usage warnings in alert email.			
Option	Description									
<i>enable</i>	Enable disk usage warnings in alert email.									
<i>disable</i>	Disable disk usage warnings 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><i>enable</i></td><td>Enable FortiCloud log quota warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud log quota warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.	<i>disable</i>	Disable FortiCloud log quota warnings in alert email.			
Option	Description									
<i>enable</i>	Enable FortiCloud log quota warnings in alert email.									
<i>disable</i>	Disable FortiCloud log quota warnings in alert email.									

Parameter	Description	Type	Size	Default						
amc-interface-bypass-mode	Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.</td></tr></table>	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.			
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.									
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><i>enable</i></td><td>Enable FIPS and Common Criteria error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FIPS and Common Criteria error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.	<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.			
Option	Description									
<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.									
<i>disable</i>	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><i>enable</i></td><td>Enable logging of FSSO collector agent disconnect.</td></tr><tr><td><i>disable</i></td><td>Disable logging of FSSO collector agent disconnect.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of FSSO collector agent disconnect.	<i>disable</i>	Disable logging of FSSO collector agent disconnect.			
Option	Description									
<i>enable</i>	Enable logging of FSSO collector agent disconnect.									
<i>disable</i>	Disable logging of FSSO collector agent disconnect.									
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.									
fpx-license-logs	Enable/disable FortiProxy license related logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiProxy license related warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiProxy license related warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiProxy license related warnings in alert email.	<i>disable</i>	Disable FortiProxy license related warnings in alert email.			
Option	Description									
<i>enable</i>	Enable FortiProxy license related warnings in alert email.									
<i>disable</i>	Disable FortiProxy license related warnings in alert email.									
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						

Parameter	Description	Type	Size	Default
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	1
alert-interval	Alert alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	2
critical-interval	Critical alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	3
error-interval	Error alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	5
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	10
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	20
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	30
debug-interval	Debug alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	60
severity	Lowest severity level to log.	option	-	alert

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.		

antivirus

This section includes syntax for the following commands:

- [config antivirus exempt-list on page 82](#)
- [config antivirus profile on page 83](#)
- [config antivirus quarantine on page 113](#)
- [config antivirus settings on page 117](#)

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-type [md5|sha1|...]
    set hash {string}
    set status [disable|enable]
  next
end
```

config antivirus exempt-list

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

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 comment {var-string}
    set replacemsg-group {string}
    set fortisandbox-mode [inline|analytics-suspicious|...]
    set fortisandbox-max-upload {integer}
    set analytics-ignore-filetype {integer}
    set analytics-accept-filetype {integer}
    set analytics-db [disable|enable]
    set mobile-malware-db [disable|enable]
  config http
    Description: Configure HTTP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set content-disarm [disable|enable]
  end
  config ftp
    Description: Configure FTP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
  end
  config imap
```

```

Description: Configure IMAP AntiVirus options.
set av-scan [disable|block|...]
set outbreak-prevention [disable|block|...]
set external-blocklist [disable|block|...]
set fortindr [disable|block|...]
set fortisandbox [disable|block|...]
set quarantine [disable|enable]
set archive-block {option1}, {option2}, ...
set archive-log {option1}, {option2}, ...
set emulator [enable|disable]
set executables [default|virus]
set content-disarm [disable|enable]
end
config pop3
Description: Configure POP3 AntiVirus options.
set av-scan [disable|block|...]
set outbreak-prevention [disable|block|...]
set external-blocklist [disable|block|...]
set fortindr [disable|block|...]
set fortisandbox [disable|block|...]
set quarantine [disable|enable]
set archive-block {option1}, {option2}, ...
set archive-log {option1}, {option2}, ...
set emulator [enable|disable]
set executables [default|virus]
set content-disarm [disable|enable]
end
config smtp
Description: Configure SMTP AntiVirus options.
set av-scan [disable|block|...]
set outbreak-prevention [disable|block|...]
set external-blocklist [disable|block|...]
set fortindr [disable|block|...]
set fortisandbox [disable|block|...]
set quarantine [disable|enable]
set archive-block {option1}, {option2}, ...
set archive-log {option1}, {option2}, ...
set emulator [enable|disable]
set executables [default|virus]
set content-disarm [disable|enable]
end
config mapi
Description: Configure MAPI AntiVirus options.
set av-scan [disable|block|...]
set outbreak-prevention [disable|block|...]
set external-blocklist [disable|block|...]
set fortindr [disable|block|...]
set fortisandbox [disable|block|...]
set quarantine [disable|enable]
set archive-block {option1}, {option2}, ...
set archive-log {option1}, {option2}, ...
set emulator [enable|disable]

```



```

    set executables [default|virus]
end
config nntp
    Description: Configure NNTP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
end
config cifs
    Description: Configure CIFS AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
end
config ssh
    Description: Configure SFTP and SCP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
end
config nac-quar
    Description: Configure AntiVirus quarantine settings.
    set infected [none|quar-src-ip]
    set expiry {user}
    set log [enable|disable]
end
config content-disarm
    Description: AV Content Disarm and Reconstruction settings.
    set original-file-destination [fortisandbox|quarantine|...]
    set error-action [block|log-only|...]
    set office-macro [disable|enable]
    set office-hylink [disable|enable]
    set office-linked [disable|enable]
    set office-embed [disable|enable]

```

```

set office-dde [disable|enable]
set office-action [disable|enable]
set pdf-javacode [disable|enable]
set pdf-embedfile [disable|enable]
set pdf-hyperlink [disable|enable]
set pdf-act-gotor [disable|enable]
set pdf-act-launch [disable|enable]
set pdf-act-sound [disable|enable]
set pdf-act-movie [disable|enable]
set pdf-act-java [disable|enable]
set pdf-act-form [disable|enable]
set cover-page [disable|enable]
set detect-only [disable|enable]
end
set outbreak-prevention-archive-scan [disable|enable]
set external-blocklist-enable-all [disable|enable]
set external-blocklist <name1>, <name2>, ...
set ems-threat-feed [disable|enable]
set fortindr-error-action [log-only|block|...]
set fortindr-timeout-action [log-only|block|...]
set fortisandbox-error-action [log-only|block|...]
set fortisandbox-timeout-action [log-only|block|...]
set av-virus-log [enable|disable]
set scan-mode [default|legacy]
next
end

```

config antivirus profile

Parameter	Description	Type	Size	Default								
name	Profile name.	string	Maximum length: 35									
comment	Comment.	var-string	Maximum length: 255									
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35									
fortisandbox-mode	FortiSandbox scan modes.	option	-	analytics-everything								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inline</i></td><td>FortiSandbox inline scan.</td></tr><tr><td><i>analytics-suspicious</i></td><td>FortiSandbox post-transfer scan: submit supported files if heuristics or other methods determine they are suspicious.</td></tr><tr><td><i>analytics-everything</i></td><td>FortiSandbox post-transfer scan: submit supported files and known infected files.</td></tr></table>				Option	Description	<i>inline</i>	FortiSandbox inline scan.	<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 and known infected files.
Option	Description											
<i>inline</i>	FortiSandbox inline scan.											
<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 and known infected files.											

Parameter	Description	Type	Size	Default						
fortisandbox-max-upload	Maximum size of files that can be uploaded to FortiSandbox in Mbytes.	integer	Minimum value: 1 Maximum value: 4095	10						
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	0						
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Use only the standard AV signature databases.</td></tr><tr><td>enable</td><td>Also use the FortiSandbox signature database.</td></tr></table>				Option	Description	disable	Use only the standard AV signature databases.	enable	Also use the FortiSandbox signature database.
Option	Description									
disable	Use only the standard AV signature databases.									
enable	Also use the FortiSandbox signature database.									
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not use the mobile malware signature database.</td></tr><tr><td>enable</td><td>Also use the mobile malware signature database.</td></tr></table>				Option	Description	disable	Do not use the mobile malware signature database.	enable	Also use the mobile malware signature database.
Option	Description									
disable	Do not use the mobile malware signature database.									
enable	Also use the mobile malware signature database.									
outbreak-prevention-archive-scan	Enable/disable outbreak-prevention archive scanning.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Analyze files as sent, not the content of archives.</td></tr><tr><td>enable</td><td>Analyze files including the content of archives.</td></tr></table>				Option	Description	disable	Analyze files as sent, not the content of archives.	enable	Analyze files including the content of archives.
Option	Description									
disable	Analyze files as sent, not the content of archives.									
enable	Analyze files including the content of archives.									
external-blocklist-enable-all	Enable/disable all external blocklists.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Use configured external blocklists.		
	<i>enable</i>	Enable all external blocklists.		
external-blocklist <name>	One or more external malware block lists. External blocklist.	string	Maximum length: 79	
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.		
fortindr-error-action	Action to take if FortiNDR encounters an error.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Log FortiNDR error, but allow the file.		
	<i>block</i>	Block the file on FortiNDR error.		
	<i>ignore</i>	Do nothing on FortiNDR error.		
fortindr-timeout-action	Action to take if FortiNDR encounters a scan timeout.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Log FortiNDR scan timeout, but allow the file.		
	<i>block</i>	Block the file on FortiNDR scan timeout.		
	<i>ignore</i>	Do nothing on FortiNDR scan timeout.		
fortisandbox-error-action	Action to take if FortiSandbox inline scan encounters an error.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Log FortiSandbox inline scan error, but allow the file.		
	<i>block</i>	Block the file on FortiSandbox inline scan error.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ignore</i>	Do nothing on FortiSandbox inline scan error.		
	<i>log-only</i>	Log FortiSandbox inline scan timeout, but allow the file.		
	<i>block</i>	Block the file on FortiSandbox inline scan timeout.		
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.		
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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.		

config http

Parameter	Description	Type	Size	Default
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.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
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.		
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.		
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.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></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 FortiProxy cannot open.</td></tr></table>	Option	Description	<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 FortiProxy cannot open.									
	Option	Description																				
	<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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					
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.																					

config ftp

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<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.																					
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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					

config imap

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<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.																					
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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					

Parameter	Description	Type	Size	Default						
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.									
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.									

config pop3

Parameter	Description	Type	Size	Default
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.		
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.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	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.		
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.		
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.		
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 FortiProxy cannot open.		

Parameter	Description	Type	Size	Default																		
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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					
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.																					
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.																					

config smtp

Parameter	Description	Type	Size	Default								
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.											
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.											
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.											
quarantine	Enable/disable quarantine for infected files.	option	-	disable								

Parameter	Description	Type	Size	Default																		
	<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.																					
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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					

Parameter	Description	Type	Size	Default						
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>default</td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td>virus</td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	default	Perform standard AntiVirus scanning of Windows executable files.	virus	Treat Windows executables as viruses.			
Option	Description									
default	Perform standard AntiVirus scanning of Windows executable files.									
virus	Treat Windows executables as viruses.									
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>disable</td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td>enable</td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	disable	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	enable	Enable Content Disarm and Reconstruction when performing AntiVirus scan.			
Option	Description									
disable	Disable Content Disarm and Reconstruction when performing AntiVirus scan.									
enable	Enable Content Disarm and Reconstruction when performing AntiVirus scan.									

config mapi

Parameter	Description	Type	Size	Default
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.		
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.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	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.		
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.		
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.		
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 FortiProxy cannot open.		

Parameter	Description	Type	Size	Default																		
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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					
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.																					

config nntp

Parameter	Description	Type	Size	Default								
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.											
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.		
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.		
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.		
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></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 FortiProxy cannot open.</td></tr></table>	Option	Description	<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 FortiProxy cannot open.							
	Option	Description																				
	<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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					

config cifs

Parameter	Description	Type	Size	Default								
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.											

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.											
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.											
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.											
archive-block	Select the archive types to block.	option	-									

Parameter	Description	Type	Size	Default
	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 FortiProxy 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 FortiProxy cannot open.		
emulator	Enable/disable the virus emulator.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		

config ssh

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable

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

Parameter	Description	Type	Size	Default																		
	<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.																					
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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy cannot open.																					
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.																					

config nac-quar

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

config content-disarm

Parameter	Description	Type	Size	Default								
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><i>fortisandbox</i></td><td>Send original file to configured FortiSandbox.</td></tr><tr><td><i>quarantine</i></td><td>Send original file to quarantine.</td></tr><tr><td><i>discard</i></td><td>Original file will be discarded after content disarm.</td></tr></table>	Option	Description	<i>fortisandbox</i>	Send original file to configured FortiSandbox.	<i>quarantine</i>	Send original file to quarantine.	<i>discard</i>	Original file will be discarded after content disarm.			
Option	Description											
<i>fortisandbox</i>	Send original file to configured FortiSandbox.											
<i>quarantine</i>	Send original file to quarantine.											
<i>discard</i>	Original file will be discarded after content disarm.											
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block file on CDR error.</td></tr><tr><td><i>log-only</i></td><td>Log CDR error, but allow file.</td></tr><tr><td><i>ignore</i></td><td>Do nothing on CDR error.</td></tr></table>	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.			
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-macro	Enable/disable stripping of macros in Microsoft Office documents.	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.		
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.		
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-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-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.		

Parameter	Description	Type	Size	Default						
pdf-javacode	Enable/disable stripping of JavaScript code in 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-embedfile	Enable/disable stripping of embedded files in 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-hyperlink	Enable/disable stripping of hyperlinks from 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-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-launch	Enable/disable stripping of PDF document actions that launch other applications.	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-sound	Enable/disable stripping of PDF document actions that play a sound.	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.									

Parameter	Description	Type	Size	Default						
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	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><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									
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><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.			
Option	Description									
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.									
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.									

config antivirus quarantine

Configure quarantine options.

```
config antivirus quarantine
  Description: Configure quarantine options.
```

```

set agelimit {integer}
set maxfilesize {integer}
set quarantine-quota {integer}
set drop-infected {option1}, {option2}, ...
set store-infected {option1}, {option2}, ...
set drop-machine-learning {option1}, {option2}, ...
set store-machine-learning {option1}, {option2}, ...
set lowspace [drop-new|ovrw-old]
set destination [NULL|disk|...]
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
maxfilesize	Maximum file size to quarantine (0 - 500 Mbytes, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 500	0
quarantine-quota	The amount of disk space to reserve for quarantining files (0 - 4294967295 Mbytes, depends on disk space).	integer	Minimum value: 0 Maximum value: 4294967295	0
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.	
	nnntp		NNTP.	
	imaps		IMAPS.	

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<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.																	
	Option	Description																																
	<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.																																
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																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	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.			
	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																														
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>nnntp</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.	nnntp	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.																																
	nnntp	NNTP.																																
	imaps	IMAPS.																																
	smtps	SMTPS.																																
	pop3s	POP3S.																																
	https	HTTPS.																																
	ftps	FTPS.																																
	mapi	MAPI.																																
cifs	CIFS.																																	
ssh	SSH.																																	
store-machine-learning	Quarantine files detected by machine learning found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nnntp imaps smtps pop3s https ftps mapi cifs ssh																														
	<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></table>	Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.																							
	Option	Description																																
	imap	IMAP.																																
	smtp	SMTP.																																
pop3	POP3.																																	
http	HTTP.																																	

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>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<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.			
	Option	Description																								
	<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.																									
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><i>drop-new</i></td><td>Drop (delete) the most recently quarantined files.</td></tr><tr><td><i>ovrw-old</i></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	<i>drop-new</i>	Drop (delete) the most recently quarantined files.	<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																			
	Option	Description																								
	<i>drop-new</i>	Drop (delete) the most recently quarantined files.																								
<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																									
destination	Choose whether to quarantine files to the FortiProxy disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	disk																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>NULL</i></td><td>Files that would be quarantined are deleted.</td></tr><tr><td><i>disk</i></td><td>Quarantine files to the FortiProxy hard disk.</td></tr><tr><td><i>FortiAnalyzer</i></td><td>FortiAnalyzer</td></tr></table>	Option	Description	<i>NULL</i>	Files that would be quarantined are deleted.	<i>disk</i>	Quarantine files to the FortiProxy hard disk.	<i>FortiAnalyzer</i>	FortiAnalyzer																	
	Option	Description																								
	<i>NULL</i>	Files that would be quarantined are deleted.																								
	<i>disk</i>	Quarantine files to the FortiProxy hard disk.																								
<i>FortiAnalyzer</i>	FortiAnalyzer																									

config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
  Description: Configure AntiVirus settings.
  set machine-learning-detection [enable|monitor|...]
  set use-extreme-db [enable|disable]
```

```

set grayware [enable|disable]
set override-timeout {integer}
set cache-infected-result [enable|disable]
end

```

config antivirus settings

Parameter	Description	Type	Size	Default								
machine-learning-detection	Use machine learning based malware detection.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable machine learning based malware detection.</td></tr><tr><td><i>monitor</i></td><td>Enable machine learning based malware detection for monitoring only.</td></tr><tr><td><i>disable</i></td><td>Disable machine learning based malware detection.</td></tr></table>	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.			
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.											
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable extreme AVDB.</td></tr><tr><td><i>disable</i></td><td>Disable extreme AVDB.</td></tr></table>	Option	Description	<i>enable</i>	Enable extreme AVDB.	<i>disable</i>	Disable extreme AVDB.					
Option	Description											
<i>enable</i>	Enable extreme AVDB.											
<i>disable</i>	Disable extreme AVDB.											
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable grayware detection.</td></tr><tr><td><i>disable</i></td><td>Disable grayware detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable grayware detection.	<i>disable</i>	Disable grayware detection.					
Option	Description											
<i>enable</i>	Enable grayware detection.											
<i>disable</i>	Disable grayware 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								
cache-infected-result	Enable/disable cache of infected scan results (default = enable).	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable cache of infected scan results.		
	<i>disable</i>	Disable cache of infected scan results.		

application

This section includes syntax for the following commands:

- [config application custom on page 120](#)
- [config application group on page 121](#)
- [config application list on page 122](#)
- [config application name on page 131](#)
- [config application rule-settings on page 133](#)

config application custom

Configure custom application signatures.

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

config application custom

Parameter	Description	Type	Size	Default
tag	Signature tag.	string	Maximum length: 63	
id	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095	
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Custom application signature protocol.	user	Not Specified	
technology	Custom application signature technology.	user	Not Specified	
behavior	Custom application signature behavior.	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 comment {var-string}
        set type [application|filter]
        set application <id1>, <id2>, ...
        set category <id1>, <id2>, ...
        set risk <level1>, <level2>, ...
        set protocols {user}
        set vendor {user}
        set technology {user}
        set behavior {user}
        set popularity {option1}, {option2}, ...
    next
end

```

config application group

Parameter	Description	Type	Size	Default
name	Application group name.	string	Maximum length: 63	
comment	Comments.	var-string	Maximum length: 255	
type	Application group type.	option	-	application

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>application</i></td><td>Application ID.</td></tr><tr><td><i>filter</i></td><td>Application filter.</td></tr></table>	Option	Description	<i>application</i>	Application ID.	<i>filter</i>	Application filter.									
	Option	Description														
	<i>application</i>	Application ID.														
<i>filter</i>	Application filter.															
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
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													
protocols	Application protocol filter.	user	Not Specified	all												
vendor	Application vendor filter.	user	Not Specified	all												
technology	Application technology filter.	user	Not Specified	all												
behavior	Application behavior filter.	user	Not Specified	all												
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.															

config application list

Configure application control lists.

```

config application list
    Description: Configure application control lists.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set extended-log [enable|disable]
        set other-application-action [pass|block]
        set app-replacemsg [disable|enable]
        set other-application-log [disable|enable]
        set enforce-default-app-port [disable|enable]
        set force-inclusion-ssl-di-sigs [disable|enable]
        set unknown-application-action [pass|block]
        set unknown-application-log [disable|enable]
        set p2p-block-list {option1}, {option2}, ...
        set deep-app-inspection [disable|enable]
        set options {option1}, {option2}, ...
    config entries
        Description: Application list entries.
        edit <id>
            set risk <level1>, <level2>, ...
            set category <id1>, <id2>, ...
            set application <id1>, <id2>, ...
            set protocols {user}
            set vendor {user}
            set technology {user}
            set behavior {user}
            set popularity {option1}, {option2}, ...
            set exclusion <id1>, <id2>, ...
        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 action [pass|block|...]
        set log [disable|enable]
        set log-packet [disable|enable]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        set session-ttl {integer}
        set shaper {string}
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]

```

```

        next
    end
    set control-default-network-services [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
next
end

```

config application list

Parameter	Description	Type	Size	Default
name	List name.	string	Maximum length: 35	
comment	Comments.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
extended-log	Enable/disable extended logging.	option	-	disable
	Option		Description	
	enable	Enable setting.		
	disable	Disable setting.		
other-application-action	Action for other applications.	option	-	pass
	Option		Description	
	pass	Allow sessions matching an application in this application list.		
	block	Block sessions matching an application in this application list.		
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable
	Option		Description	
	disable	Disable replacement messages for blocked applications.		
	enable	Enable replacement messages for blocked applications.		

Parameter	Description	Type	Size	Default						
other-application-log	Enable/disable logging for other applications.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging for other applications.</td></tr><tr><td><i>enable</i></td><td>Enable logging for other applications.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging for other applications.	<i>enable</i>	Enable logging for other applications.			
Option	Description									
<i>disable</i>	Disable logging for other applications.									
<i>enable</i>	Enable logging for other applications.									
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.									
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.									
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow unknown applications.</td></tr><tr><td><i>block</i></td><td>Drop or block unknown applications.</td></tr></table>	Option	Description	<i>pass</i>	Pass or allow unknown applications.	<i>block</i>	Drop or block unknown applications.			
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging for unknown applications.</td></tr><tr><td><i>enable</i></td><td>Enable logging for unknown applications.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging for unknown applications.	<i>enable</i>	Enable logging for unknown applications.			
Option	Description									
<i>disable</i>	Disable logging for unknown applications.									
<i>enable</i>	Enable logging for unknown applications.									

Parameter	Description	Type	Size	Default										
p2p-block-list	P2P applications to be block listed.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>skype</td><td>Skype.</td></tr><tr><td>edonkey</td><td>Edonkey.</td></tr><tr><td>bittorrent</td><td>Bit torrent.</td></tr></table>	Option	Description	skype	Skype.	edonkey	Edonkey.	bittorrent	Bit torrent.					
Option	Description													
skype	Skype.													
edonkey	Edonkey.													
bittorrent	Bit torrent.													
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.													
options	Basic application protocol signatures allowed by default.	option	-	allow-dns										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow-dns</td><td>Allow DNS.</td></tr><tr><td>allow-icmp</td><td>Allow ICMP.</td></tr><tr><td>allow-http</td><td>Allow generic HTTP web browsing.</td></tr><tr><td>allow-ssl</td><td>Allow generic SSL communication.</td></tr></table>	Option	Description	allow-dns	Allow DNS.	allow-icmp	Allow ICMP.	allow-http	Allow generic HTTP web browsing.	allow-ssl	Allow generic SSL communication.			
Option	Description													
allow-dns	Allow DNS.													
allow-icmp	Allow ICMP.													
allow-http	Allow generic HTTP web browsing.													
allow-ssl	Allow generic SSL communication.													
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.													

config entries

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

Parameter	Description	Type	Size	Default												
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													
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295													
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
protocols	Application protocol filter.	user	Not Specified	all												
vendor	Application vendor filter.	user	Not Specified	all												
technology	Application technology filter.	user	Not Specified	all												
behavior	Application behavior filter.	user	Not Specified	all												
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.															
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
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.		
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.		
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous
	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
	Option	Description		
	<i>none</i>	none		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dhcp-client-mac</i>	DHCP client.		
	<i>dns-domain</i>	DNS domain.		
session-ttl	Session TTL (0 = default).	integer	Minimum value: 0 Maximum value: 4294967295	0
shaper	Traffic shaper.	string	Maximum length: 35	
quarantine	Quarantine method.	option	-	none
	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
	Option	Description		
	<i>disable</i>	Disable quarantine logging.		
	<i>enable</i>	Enable quarantine logging.		

config parameters

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

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 default-network-services

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
port	Port number.	integer	Minimum value: 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.		

Parameter	Description	Type	Size	Default
violation-action	Action for protocols not in the allowlist for selected port.	option	-	block
	Option	Description		
	<i>pass</i>	Allow protocols not in the allowlist for selected port.		
	<i>monitor</i>	Monitor protocols not in the allowlist for selected port.		
	<i>block</i>	Block protocols not in the allowlist for selected port.		

config application name

Configure application signatures.

```

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

```

config application name

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

config parameters

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

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config application rule-settings

Configure application rule settings.

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

config application rule-settings

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

authentication

This section includes syntax for the following commands:

- [config authentication rule on page 134](#)
- [config authentication scheme on page 137](#)
- [config authentication setting on page 140](#)

config authentication rule

Configure Authentication Rules.

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

config authentication rule

Parameter	Description	Type	Size	Default
name	Authentication rule name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default												
status	Enable/disable this authentication rule.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this authentication rule.</td></tr><tr><td><i>disable</i></td><td>Disable this authentication rule.</td></tr></table>	Option	Description	<i>enable</i>	Enable this authentication rule.	<i>disable</i>	Disable this authentication rule.									
	Option	Description														
	<i>enable</i>	Enable this authentication rule.														
<i>disable</i>	Disable this authentication rule.															
protocol	Authentication is required for the selected protocol (default = HTTP).	option	-	http												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP traffic is matched and authentication is required.</td></tr><tr><td><i>ftp</i></td><td>FTP traffic is matched and authentication is required.</td></tr><tr><td><i>socks</i></td><td>SOCKS traffic is matched and authentication is required.</td></tr><tr><td><i>ssh</i></td><td>SSH traffic is matched and authentication is required.</td></tr><tr><td><i>ztna-portal</i></td><td>ZTNA portal traffic is matched and authentication is required.</td></tr></table>	Option	Description	<i>http</i>	HTTP traffic is matched and authentication is required.	<i>ftp</i>	FTP traffic is matched and authentication is required.	<i>socks</i>	SOCKS traffic is matched and authentication is required.	<i>ssh</i>	SSH traffic is matched and authentication is required.	<i>ztna-portal</i>	ZTNA portal traffic is matched and authentication is required.			
	Option	Description														
	<i>http</i>	HTTP traffic is matched and authentication is required.														
	<i>ftp</i>	FTP traffic is matched and authentication is required.														
	<i>socks</i>	SOCKS traffic is matched and authentication is required.														
	<i>ssh</i>	SSH traffic is matched and authentication is required.														
<i>ztna-portal</i>	ZTNA portal traffic is matched and authentication is required.															
web-proxy	Web-Proxy profile.	string	Maximum length: 35													
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79													
srcaddr <name>	Authentication is required for the selected IPv4 source address. Address name.	string	Maximum length: 79													
dstaddr <name>	Select an IPv4 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79													
srcaddr6 <name>	Authentication is required for the selected IPv6 source address. 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												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IP-based authentication.		
	<i>disable</i>	Disable IP-based authentication.		
active-auth-method	Select an active authentication method.	string	Maximum length: 35	
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35	
web-auth-cookie	Enable/disable Web authentication cookies (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Web authentication cookie.		
	<i>disable</i>	Disable Web authentication cookie.		
cors-stateful	Enable/disable allowance of CORS access (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable allowance of CORS access		
	<i>disable</i>	Disable allowance of CORS access		
cors-depth	Depth to allow CORS access (default = 3).	integer	Minimum value: 1 Maximum value: 8	3
cert-auth-cookie	Enable/disable to use device certificate as authentication cookie (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable device certificate as authentication cookie.		
	<i>disable</i>	Disable device certificate as authentication cookie.		
transaction-based	Enable/disable transaction based authentication (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable transaction based authentication.		
	<i>disable</i>	Disable transaction based authentication.		

Parameter	Description	Type	Size	Default						
web-portal	Enable/disable web portal for proxy transparent policy (default = enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable web-portal.</td></tr><tr><td><i>disable</i></td><td>Disable web-portal.</td></tr></table>				Option	Description	<i>enable</i>	Enable web-portal.	<i>disable</i>	Disable web-portal.
Option	Description									
<i>enable</i>	Enable web-portal.									
<i>disable</i>	Disable web-portal.									
comments	Comment.	var-string	Maximum length: 1023							
form-auth-fallback	Enable/disable to use FORM authentication if needed.(default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Form Authentication Fallback</td></tr><tr><td><i>disable</i></td><td>Disable Form Authentication Fallback</td></tr></table>				Option	Description	<i>enable</i>	Enable Form Authentication Fallback	<i>disable</i>	Disable Form Authentication Fallback
Option	Description									
<i>enable</i>	Enable Form Authentication Fallback									
<i>disable</i>	Disable Form Authentication Fallback									

config authentication scheme

Configure Authentication Schemes.

```

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

```

config authentication scheme

Parameter	Description	Type	Size	Default																												
name	Authentication scheme name.	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>rsso</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>x-auth-user</i></td><td>User from HTTP x-authenticated-user header.</td></tr><tr><td><i>ztna-relay</i></td><td>ZTNA relay authentication.</td></tr><tr><td><i>oidc</i></td><td>OpenID Connect.</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>rsso</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>x-auth-user</i>	User from HTTP x-authenticated-user header.	<i>ztna-relay</i>	ZTNA relay authentication.	<i>oidc</i>	OpenID Connect.			
	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>rsso</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>x-auth-user</i>	User from HTTP x-authenticated-user header.																														
	<i>ztna-relay</i>	ZTNA relay authentication.																														
<i>oidc</i>	OpenID Connect.																															
negotiate-ntlm	Enable/disable negotiate authentication for NTLM (default = disable).	option	-	enable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negotiate authentication for NTLM.</td></tr><tr><td><i>disable</i></td><td>Disable negotiate authentication for NTLM.</td></tr></table>	Option	Description	<i>enable</i>	Enable negotiate authentication for NTLM.	<i>disable</i>	Disable negotiate authentication for NTLM.																									
	Option	Description																														
	<i>enable</i>	Enable negotiate authentication for NTLM.																														
<i>disable</i>	Disable negotiate authentication for NTLM.																															
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35																													
domain-controller	Domain controller setting.	string	Maximum length: 35																													
saml-server	SAML configuration.	string	Maximum length: 35																													

Parameter	Description	Type	Size	Default						
saml-timeout	SAML authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120						
oidc-server <name>	OpenID Connect servers configuration. OpenID Connect server list.	string	Maximum length: 79							
oidc-timeout	OpenID Connect authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120						
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35							
require-tfa	Enable/disable two-factor authentication (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable two-factor authentication.</td></tr><tr><td>disable</td><td>Disable two-factor authentication.</td></tr></table>				Option	Description	enable	Enable two-factor authentication.	disable	Disable two-factor authentication.
Option	Description									
enable	Enable two-factor authentication.									
disable	Disable two-factor authentication.									
fsso-guest	Enable/disable user fsso-guest authentication (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable user fsso-guest authentication.</td></tr><tr><td>disable</td><td>Disable user fsso-guest authentication.</td></tr></table>				Option	Description	enable	Enable user fsso-guest authentication.	disable	Disable user fsso-guest authentication.
Option	Description									
enable	Enable user fsso-guest authentication.									
disable	Disable user fsso-guest authentication.									
user-cert	Enable/disable authentication with user certificate (default = disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable client certificate field authentication.</td></tr><tr><td>disable</td><td>Disable client certificate field authentication.</td></tr></table>				Option	Description	enable	Enable client certificate field authentication.	disable	Disable client certificate field authentication.
Option	Description									
enable	Enable client certificate field authentication.									
disable	Disable client certificate field authentication.									
search-all-ldap-databases	Enable/disable searching all LDAP databases to find groups.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable searching for groups in all LDAP databases.</td></tr><tr><td>disable</td><td>Disable searching for groups in all LDAP databases.</td></tr></table>				Option	Description	enable	Enable searching for groups in all LDAP databases.	disable	Disable searching for groups in all LDAP databases.
Option	Description									
enable	Enable searching for groups in all LDAP databases.									
disable	Disable searching for groups in all LDAP databases.									

Parameter	Description	Type	Size	Default						
user-database <name>	Authentication server to contain user information; "local" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79							
digest-algo	Digest Authentication Algorithms.	option	-	md5 sha-256						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>sha-256</i></td><td>SHA-256.</td></tr></table>				Option	Description	<i>md5</i>	MD5.	<i>sha-256</i>	SHA-256.
Option	Description									
<i>md5</i>	MD5.									
<i>sha-256</i>	SHA-256.									
ssh-ca	SSH CA name.	string	Maximum length: 35							

config authentication setting

Configure authentication setting.

```

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

```


config authentication setting

Parameter	Description	Type	Size	Default						
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35							
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35							
update-time	Time of the last update.	user	Not Specified							
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><i>enable</i></td><td>Enable persistent cookie.</td></tr><tr><td><i>disable</i></td><td>Disable persistent cookie.</td></tr></table>				Option	Description	<i>enable</i>	Enable persistent cookie.	<i>disable</i>	Disable persistent cookie.
Option	Description									
<i>enable</i>	Enable persistent cookie.									
<i>disable</i>	Disable persistent cookie.									
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><i>enable</i></td><td>Enable persistent cookie for IP-based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable persistent cookie for IP-based authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable persistent cookie for IP-based authentication.	<i>disable</i>	Disable persistent cookie for IP-based authentication.
Option	Description									
<i>enable</i>	Enable persistent cookie for IP-based authentication.									
<i>disable</i>	Disable persistent cookie for IP-based authentication.									
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						
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						
captive-portal-type	Captive portal type.	option	-	fqdn						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fqdn</i></td><td>Use FQDN for captive portal.</td></tr><tr><td><i>ip</i></td><td>Use an IP address for captive portal.</td></tr></table>				Option	Description	<i>fqdn</i>	Use FQDN for captive portal.	<i>ip</i>	Use an IP address for captive portal.
Option	Description									
<i>fqdn</i>	Use FQDN for captive portal.									
<i>ip</i>	Use an IP address for captive portal.									

Parameter	Description	Type	Size	Default						
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	::						
captive-portal	Captive portal host name.	string	Maximum length: 255							
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255							
cert-auth	Enable/disable redirecting certificate authentication to HTTPS portal.	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.									
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						
captive-portal-port	Captive portal port number (1 - 65535, default = 7830).	integer	Minimum value: 1 Maximum value: 65535	7830						
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	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
captive-portal-ssl-port	Captive portal SSL port number (1 - 65535, default = 7831).	integer	Minimum value: 1 Maximum value: 65535	7831
user-cert-ca <name>	CA certificate used for client certificate verification. CA certificate list.	string	Maximum length: 79	
dev-range <name>	Address range for the IP based device query. Address name.	string	Maximum length: 79	
log-auth-request	Enable/disable to log authentication request.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	

automation

This section includes syntax for the following commands:

- [config automation setting on page 144](#)

config automation setting

Automation setting configuration.

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

config automation setting

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

casb

This section includes syntax for the following commands:

- [config casb profile on page 145](#)
- [config casb saas-application on page 148](#)
- [config casb user-activity on page 149](#)

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>
        set status [enable|disable]
        set safe-search [enable|disable]
        set safe-search-control <name1>, <name2>, ...
        set tenant-control [enable|disable]
        set tenant-control-tenants <name1>, <name2>, ...
        set domain-control [enable|disable]
        set domain-control-domains <name1>, <name2>, ...
        set log [enable|disable]
        config access-rule
          Description: CASB profile access rule.
          edit <name>
            set action [monitor|bypass|...]
            set bypass {option1}, {option2}, ...
          next
        end
      config custom-control
        Description: CASB profile custom control.
        edit <name>
          config option
            Description: CASB custom control option.
            edit <name>
              set user-input <value1>, <value2>, ...
            next
          end
        next
      end
    next
  end
next
```

```
end
next
end
```

config casb profile

Parameter	Description	Type	Size	Default
name	CASB profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	

config saas-application

Parameter	Description	Type	Size	Default						
name	CASB profile 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.									
safe-search	Enable/disable safe search.	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-control <name>	CASB profile safe search control. Safe search control name.	string	Maximum length: 79							
tenant-control	Enable/disable tenant control.	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						
tenant-control-tenants <name>	CASB profile tenant control tenants. Tenant control tenants name.	string	Maximum length: 79							
domain-control	Enable/disable domain control.	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.									
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><i>enable</i></td><td>Enable log setting.</td></tr><tr><td><i>disable</i></td><td>Disable log setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable log setting.	<i>disable</i>	Disable log setting.			
Option	Description									
<i>enable</i>	Enable log setting.									
<i>disable</i>	Disable log setting.									

config access-rule

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>web-filter</i>	Exempt from web filter.		
	<i>file-filter</i>	Exempt from file filter.		
	<i>video-filter</i>	Exempt from video filter.		

config custom-control

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

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 uuid {string}
    set status [enable|disable]
    set type [built-in|customized]
    set casb-name {string}
    set description {string}
    set domains <domain1>, <domain2>, ...
  next
end

```


config casb saas-application

Parameter	Description	Type	Size	Default						
name	SaaS application name.	string	Maximum length: 79							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 36							
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.									
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							

config casb user-activity

Configure CASB user activity.

```
config casb user-activity
  Description: Configure CASB user activity.
  edit <name>
    set uuid {string}
    set status [enable|disable]
    set description {string}
    set type [built-in|customized]
    set casb-name {string}
    set application {string}
    set category [activity-control|tenant-control|...]
    set match-strategy [and|or]
    config match
```

```

Description: CASB user activity match rules.
edit <id>
    set strategy [and|or]
    config rules
        Description: CASB user activity rules.
        edit <id>
            set type [domains|host|...]
            set domains <domain1>, <domain2>, ...
            set methods <method1>, <method2>, ...
            set match-pattern [simple|substr|...]
            set match-value {string}
            set header-name {string}
            set case-sensitive [enable|disable]
            set negate [enable|disable]
        next
    end
next
end
config control-options
    Description: CASB control options.
    edit <name>
        set status [enable|disable]
        config operations
            Description: CASB control option operations.
            edit <name>
                set target [header|path]
                set action [append|prepend|...]
                set direction {option}
                set header-name {string}
                set search-pattern [simple|substr|...]
                set search-key {string}
                set case-sensitive [enable|disable]
                set value-from-input [enable|disable]
                set values <value1>, <value2>, ...
            next
        end
    next
end
next
end
end

```

config casb user-activity

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

Parameter	Description	Type	Size	Default												
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 36													
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.															
description	CASB user activity description.	string	Maximum length: 63													
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.															
casb-name	CASB user activity signature name.	string	Maximum length: 79													
application	CASB SaaS application name.	string	Maximum length: 79													
category	CASB user activity category.	option	-	activity-control												
	<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.															
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.															

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
	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
id	CASB user activity rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	CASB user activity rule type.	option	-	host
	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.		
domains <domain>	CASB user activity domain list. Domain list separated by space.	string	Maximum length: 127	
methods <method>	CASB user activity method list. User activity method.	string	Maximum length: 79	
match-pattern	CASB user activity rule match pattern.	option	-	simple

Parameter	Description	Type	Size	Default
	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	
header-name	CASB user activity rule header name.	string	Maximum length: 255	
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.		
negate	Enable/disable what the matching strategy must not be.	option	-	disable
	Option Description			
	<i>enable</i>	Matching strategy is negated.		
	<i>disable</i>	Matching strategy is not negated.		

config control-options

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

config operations

Parameter	Description	Type	Size	Default														
name	CASB control option operation name.	string	Maximum length: 79															
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></table>	Option	Description	<i>header</i>	Header.	<i>path</i>	Path.											
Option	Description																	
<i>header</i>	Header.																	
<i>path</i>	Path.																	
action	CASB operation action.	option	-	append														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>append</i></td><td>Append the values after the target.</td></tr><tr><td><i>prepend</i></td><td>Prepend the values before the target.</td></tr><tr><td><i>replace</i></td><td>Replace the target by the value.</td></tr><tr><td><i>new</i></td><td>Create a new header regardless if existing header is found or not.</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>delete</i></td><td>Delete the target.</td></tr></table>	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.			
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.																	
direction	CASB operation direction.	option	-	request														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>request</i></td><td>Request.</td></tr></table>	Option	Description	<i>request</i>	Request.													
Option	Description																	
<i>request</i>	Request.																	
header-name	CASB operation header name to search.	string	Maximum length: 255															
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>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.																	
search-key	CASB operation key to search.	string	Maximum length: 1023															

Parameter	Description	Type	Size	Default
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.		
value-from-input	Enable/disable value from user input.	option	-	disable
	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	

certificate

This section includes syntax for the following commands:

- [config certificate ca on page 156](#)
- [config certificate crl on page 158](#)
- [config certificate hsm-local on page 159](#)
- [config certificate local on page 164](#)
- [config certificate remote on page 169](#)

config certificate ca

CA certificate.

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

config certificate ca

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 79	
ca	CA certificate as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the CA certificate.	option	-	global

Parameter	Description	Type	Size	Default								
	<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.											
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.											
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Trusted CA for SSL inspection.</td></tr><tr><td><i>disable</i></td><td>Untrusted CA for SSL inspection.</td></tr></table>	Option	Description	<i>enable</i>	Trusted CA for SSL inspection.	<i>disable</i>	Untrusted CA for SSL inspection.					
	Option	Description										
	<i>enable</i>	Trusted CA for SSL inspection.										
<i>disable</i>	Untrusted CA for SSL inspection.											
scep-url	URL of the SCEP server.	string	Maximum length: 255									
est-url	URL of the EST server.	string	Maximum length: 255									
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								
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0								
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255									
obsolete	Enable/disable this CA as obsoleted.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Alive.		
	<i>enable</i>	Obsolete.		
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.		

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 range [global|vdom]
    set source [factory|user|...]
    set update-vdom {string}
    set ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set http-url {string}
    set scep-url {string}
    set scep-cert {string}
    set update-interval {integer}
    set source-ip {ipv4-address}
  next
end

```

config certificate crl

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
crl	Certificate Revocation List as a PEM file.	user	Not Specified	

Parameter	Description	Type	Size	Default								
range	Either global or VDOM IP address range for the 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.											
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.											
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									
ldap-password	LDAP server user password.	password	Not Specified									
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255									
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								
update-interval	Time in seconds before the FortiProxy checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0								
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0								

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

```

config certificate hsm-local

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comments	Comment.	string	Maximum length: 511	
vendor	HSM vendor.	option	-	unknown

Option	Description
<i>unknown</i>	Unknown type of HSM.
<i>gch</i>	Google Cloud HSM.

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><i>unknown</i></td><td>Unknown API version.</td></tr><tr><td><i>gch-default</i></td><td>Google Cloud HSM default API.</td></tr></table>	Option	Description	<i>unknown</i>	Unknown API version.	<i>gch-default</i>	Google Cloud HSM default API.					
Option	Description											
<i>unknown</i>	Unknown API version.											
<i>gch-default</i>	Google Cloud HSM default API.											
certificate	PEM format certificate.	user	Not Specified									
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><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.											
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.											
gch-url	Google Cloud HSM key URL (e.g. "https://cloudkms.googleapis.com/v1/projects/sampleproject/locations/samplelocation/keyRings/samplekeyring/cryptoKeys/sampleKeyName/cryptoKeyVersions/1").	string	Maximum length: 1024									

Parameter	Description	Type	Size	Default
gch-project	Google Cloud HSM project ID.	string	Maximum length: 31	
gch-location	Google Cloud HSM location.	string	Maximum length: 63	
gch-keyring	Google Cloud HSM keyring.	string	Maximum length: 63	
gch-cryptokey	Google Cloud HSM cryptokey.	string	Maximum length: 63	
gch-cryptokey-version	Google Cloud HSM cryptokey version.	string	Maximum length: 31	
gch-cloud-service-name	Cloud service config name to generate access token.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
gch-cryptokey-algorithm	Google Cloud HSM cryptokey algorithm.	option	-	rsa-sign-pkcs1-2048-sha256

Option	Description
rsa-sign-pkcs1-2048-sha256	2048 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
rsa-sign-pkcs1-3072-sha256	3072 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
rsa-sign-pkcs1-4096-sha256	4096 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest.
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.

config certificate local

Local keys and certificates.

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


config certificate local

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 35							
type	Type.	option	-	normal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal</td></tr><tr><td><i>hsm</i></td><td>HSM</td></tr></table>				Option	Description	<i>normal</i>	Normal	<i>hsm</i>	HSM
	Option	Description								
	<i>normal</i>	Normal								
<i>hsm</i>	HSM									
password	Password as a PEM file.	password	Not Specified							
hsm-vendor	HSM vendor.	option	-	safenet						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>safenet</i></td><td>Safenet HSM.</td></tr><tr><td><i>primus</i></td><td>Securosys Primus HSM.</td></tr></table>				Option	Description	<i>safenet</i>	Safenet HSM.	<i>primus</i>	Securosys Primus HSM.
	Option	Description								
	<i>safenet</i>	Safenet HSM.								
<i>primus</i>	Securosys Primus HSM.									
hsm-slot	HSM slot to use with this certificate.	string	Maximum length: 35							
hsm-keytype	HSM certificate key type.	option	-	rsa						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rsa</i></td><td>RSA key type.</td></tr><tr><td><i>ec</i></td><td>EC key type.</td></tr></table>				Option	Description	<i>rsa</i>	RSA key type.	<i>ec</i>	EC key type.
	Option	Description								
	<i>rsa</i>	RSA key type.								
<i>ec</i>	EC key type.									
comments	Comment.	string	Maximum length: 511							
private-key	PEM format key encrypted with a password.	user	Not Specified							
certificate	PEM format certificate.	user	Not Specified							
csr	Certificate Signing Request.	user	Not Specified							
state	Certificate Signing Request State.	user	Not Specified							
scep-url	SCEP server URL.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default								
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><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.											
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.											
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								
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified									
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255									
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.											

Parameter	Description	Type	Size	Default												
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0												
ike-localid	Local ID the FortiProxy 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.															
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.															
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>enable</td><td>Keep the existing private key during SCEP renewal.</td></tr><tr><td>disable</td><td>Generate a new private key during SCEP renewal.</td></tr></table>				Option	Description	enable	Keep the existing private key during SCEP renewal.	disable	Generate a new private key during SCEP renewal.						
Option	Description															
enable	Keep the existing private key during SCEP renewal.															
disable	Generate a new private key during SCEP renewal.															
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63													
cmp-path	Path location inside CMP server.	string	Maximum length: 255													
cmp-server-cert	CMP server certificate.	string	Maximum length: 79													

Parameter	Description	Type	Size	Default
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate
	Option	Description		
	keyupate	Key Update.		
	renewal	Renewal.		
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 FortiProxy unit.	string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
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
acme-renew-window	Beginning of the renewal window (in days before certificate expiration, 30 by default).	integer	Minimum value: 1 Maximum value: 100	30
est-server	Address and port for EST server (e.g. https://example.com:1234).	string	Maximum length: 255	
est-ca-id	CA identifier of the CA server for signing via EST.	string	Maximum length: 255	
est-http-username	HTTP Authentication username for signing via EST.	string	Maximum length: 63	
est-http-password	HTTP Authentication password for signing via EST.	string	Maximum length: 63	
est-client-cert	Certificate used to authenticate this FortiGate to EST server.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
est-server-cert	EST server's certificate must be verifiable by this certificate to be authenticated.	string	Maximum length: 79							
est-srp-username	EST SRP authentication username.	string	Maximum length: 63							
est-srp-password	EST SRP authentication password.	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><i>create-new-key</i></td><td>Create new private key during re-enrollment.</td></tr><tr><td><i>use-existing-key</i></td><td>Reuse existing private key during re-enrollment.</td></tr></table>	Option	Description	<i>create-new-key</i>	Create new private key during re-enrollment.	<i>use-existing-key</i>	Reuse existing private key during re-enrollment.			
Option	Description									
<i>create-new-key</i>	Create new private key during re-enrollment.									
<i>use-existing-key</i>	Reuse existing private key during re-enrollment.									

config certificate remote

Remote certificate as a PEM file.

```

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

```

config certificate remote

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
remote	Remote certificate.	user	Not Specified	

Parameter	Description	Type	Size	Default
range	Either the global or VDOM IP address range for the remote certificate.	option	-	global
	Option	Description		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
source	Remote 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.		

dlp

This section includes syntax for the following commands:

- [config dlp data-type on page 171](#)
- [config dlp dictionary on page 173](#)
- [config dlp exact-data-match on page 175](#)
- [config dlp filepattern on page 176](#)
- [config dlp fp-doc-source on page 179](#)
- [config dlp profile on page 183](#)
- [config dlp sensitivity on page 187](#)
- [config dlp sensor on page 188](#)
- [config dlp settings on page 189](#)

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 pattern {string}
    set verify {string}
    set verify2 {string}
    set match-around {string}
    set look-back {integer}
    set look-ahead {integer}
    set match-back {integer}
    set match-ahead {integer}
    set transform {string}
    set verify-transformed-pattern [enable|disable]
    set comment {var-string}
  next
end
```

config dlp data-type

Parameter	Description	Type	Size	Default
name	Name of table containing the data type.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
pattern	Regular expression pattern string without look around.	string	Maximum length: 255							
verify	Regular expression pattern string used to verify the data type.	string	Maximum length: 255							
verify2	Extra regular expression pattern string used to verify the data type.	string	Maximum length: 255							
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							
look-back	Number of characters required to save for verification (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255	1						
look-ahead	Number of characters to obtain in advance for verification (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255	1						
match-back	Number of characters in front for match-around (1 - 4096, default = 1).	integer	Minimum value: 1 Maximum value: 4096	1						
match-ahead	Number of characters behind for match-around (1 - 4096, default = 1).	integer	Minimum value: 1 Maximum value: 4096	1						
transform	Template to transform user input to a pattern using capture group from 'pattern'.	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.									
comment	Optional comments.	var-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 uuid {uuid}
    set match-type [match-all|match-any]
    set match-around [enable|disable]
    set comment {var-string}
    config entries
      Description: DLP dictionary entries.
      edit <id>
        set type {string}
        set pattern {string}
        set ignore-case [enable|disable]
        set repeat [enable|disable]
        set status [enable|disable]
        set comment {var-string}
      next
    end
  next
end
```

config dlp dictionary

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
name	Name of table containing the dictionary.	string	Maximum length: 35	
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.		
match-around	Enable/disable match-around support.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable match-around support.		
	<i>disable</i>	Disable match-around support.		
comment	Optional comments.	var-string	Maximum length: 255	

config entries

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

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

config dlp exact-data-match

Parameter	Description	Type	Size	Default
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
data	External resource for exact data match.	string	Maximum length: 35	

config columns

Parameter	Description	Type	Size	Default
index	Column index.	integer	Minimum value: 1 Maximum value: 32	0
type	Data-type for this column.	string	Maximum length: 35	
optional	Enable/disable optional match.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable optional match.		
	<i>disable</i>	Disable optional match.		

config dlp filepattern

Configure file patterns used by DLP blocking.

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

config dlp filepattern

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

config entries

Parameter	Description	Type	Size	Default
filter-type	Filter by file name pattern or by file type.	option	-	pattern
	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	
file-type	Select a file type.	option	-	unknown
	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>hta</i>	Match hta files.		
	<i>html</i>	Match html files.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>jar</i>	Match jar files.		
	<i>jnlp</i>	Match jnlp files.		
	<i>msoffice</i>	Match MS-Office files. For example, doc, xls, ppt, and so on.		
	<i>msofficex</i>	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.		
	<i>fsg</i>	Match fsg files.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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>css</i>	Match CSS files.		
<i>com</i>	Match COM files.			

config dlp fp-doc-source

Create a DLP fingerprint database by allowing the FortiProxy 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 FortiProxy to access a file
server containing files from which to create fingerprints.
    edit <name>
        set server-type {option}
        set server {string}
        set period [none|daily|...]
        set vdom [mgmt|current]
        set scan-subdirectories [enable|disable]
        set scan-on-creation [enable|disable]
        set remove-deleted [enable|disable]
```

```

set keep-modified [enable|disable]
set username {string}
set password {password}
set file-path {string}
set file-pattern {string}
set sensitivity {string}
set tod-hour {integer}
set tod-min {integer}
set weekday [sunday|monday|...]
set date {integer}
next
end

```

config dlp fp-doc-source

Parameter	Description	Type	Size	Default										
name	Name of the DLP fingerprint database.	string	Maximum length: 35											
server-type	Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.	option	-	samba										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>samba</td><td>SAMBA server.</td></tr></table>	Option	Description	samba	SAMBA server.									
Option	Description													
samba	SAMBA server.													
server	IPv4 or IPv6 address of the server.	string	Maximum length: 35											
period	Frequency for which the FortiProxy checks the server for new or changed files.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Check the server when the FortiGate starts up.</td></tr><tr><td>daily</td><td>Check the server once a day.</td></tr><tr><td>weekly</td><td>Check the server once a week.</td></tr><tr><td>monthly</td><td>Check the server once a month.</td></tr></table>	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.			
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.													
vdom	Select the VDOM that can communicate with the file server.	option	-	mgmt										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mgmt</i>	Communicate with the file server through the management VDOM.		
	<i>current</i>	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.		
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.		
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.		
remove-deleted	Enable to keep the fingerprint database up to date when a file is deleted from the server.	option	-	enable
	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.		
keep-modified	Enable so that when a file is changed on the server the FortiProxy keeps the old fingerprint and adds a new fingerprint to the database.	option	-	enable
	Option	Description		
	<i>enable</i>	Keep the old fingerprint and add a new fingerprint when a file is changed on the server.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Replace the old fingerprint with the new fingerprint when a file is changed on the server.</td></tr></table>	Option	Description	<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.															
Option	Description																			
<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.																			
username	User name required to log into the file server.	string	Maximum length: 35																	
password	Password required to log into the file server.	password	Not Specified																	
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	*																
sensitivity	Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using sensitivity.	string	Maximum length: 35																	
tod-hour	Hour of the day on which to scan the server (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23	1																
tod-min	Minute of the hour on which to scan the server (0 - 59).	integer	Minimum value: 0 Maximum value: 59	0																
weekday	Day of the week on which to scan the server.	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																			
date	Day of the month on which to scan the server (1 - 31).	integer	Minimum value: 1 Maximum value: 31	1																

config dlp profile

Configure DLP profiles.

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

config dlp profile

Parameter	Description	Type	Size	Default
name	Name of the DLP profile.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
feature-set	Flow/proxy feature set.	option	-	proxy

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
replacemsg-group	Replacement message group used by this DLP profile.	string	Maximum length: 35	
dlp-log	Enable/disable DLP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP logging.		
	<i>disable</i>	Disable DLP logging.		
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.		
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.		
summary-proto	Protocols to always log summary.	option	-	

Parameter	Description	Type	Size	Default
	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.		

config rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Filter name.	string	Maximum length: 35	
severity	Select the severity or threat level that matches this filter.	option	-	medium
	Option		Description	
	info		Informational.	
	low		Low.	
	medium		Medium.	
	high		High.	
	critical		Critical.	
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file

Parameter	Description	Type	Size	Default																						
	<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.																									
proto	Check messages or files over one or more of these protocols.	option	-																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>http-get</i></td><td>HTTP GET.</td></tr><tr><td><i>http-post</i></td><td>HTTP POST.</td></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>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.			
	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.																									
filter-by	Select the type of content to match.	option	-	none																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sensor</i></td><td>Use DLP sensors to match content.</td></tr><tr><td><i>mip</i></td><td>Use MIP label dictionary to match content.</td></tr><tr><td><i>fingerprint</i></td><td>Match against a fingerprint sensitivity.</td></tr><tr><td><i>encrypted</i></td><td>Look for encrypted files.</td></tr><tr><td><i>none</i></td><td>No content scan.</td></tr></table>	Option	Description	<i>sensor</i>	Use DLP sensors to match content.	<i>mip</i>	Use MIP label dictionary to match content.	<i>fingerprint</i>	Match against a fingerprint sensitivity.	<i>encrypted</i>	Look for encrypted files.	<i>none</i>	No content scan.													
	Option	Description																								
	<i>sensor</i>	Use DLP sensors to match content.																								
	<i>mip</i>	Use MIP label dictionary to match content.																								
	<i>fingerprint</i>	Match against a fingerprint sensitivity.																								
	<i>encrypted</i>	Look for encrypted files.																								
<i>none</i>	No content scan.																									
file-size	Match files greater than or equal to this size (KB).	integer	Minimum value: 0 Maximum value: 4193280	0																						
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35																							

Parameter	Description	Type	Size	Default										
match-percentage	Percentage of fingerprints in the fingerprint databases designated with the selected sensitivity to match.	integer	Minimum value: 1 Maximum value: 100	10										
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0										
sensor <name>	Select DLP sensors. Address name.	string	Maximum length: 35											
label	MIP label dictionary.	string	Maximum length: 35											
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.													
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.													
expiry	Quarantine duration in days, hours, minutes (format = dddhhmm).	user	Not Specified	5m										

config dlp sensitivity

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

config dlp sensor

Parameter	Description	Type	Size	Default
name	Name of table containing the sensor.	string	Maximum length: 35	
match-type	Logical relation between entries (default = match-any).	option	-	match-any

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>match-all</i>	Match all entries.		
	<i>match-any</i>	Match any entries.		
	<i>match-eval</i>	Match an expression evaluation.		
eval	Expression to evaluate.	string	Maximum length: 255	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 1 Maximum value: 32	0						
dictionary	Select a DLP dictionary or exact-data-match.	string	Maximum length: 35							
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						
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

Designate logical storage for DLP fingerprint database.

```
config dlp settings
  Description: Designate logical storage for DLP fingerprint database.
  set storage-device {string}
  set size {integer}
  set db-mode [stop-adding|remove-modified-then-oldest|...]
  set cache-mem-percent {integer}
```

```
set chunk-size {integer}
end
```

config dlp settings

Parameter	Description	Type	Size	Default								
storage-device	Storage device name.	string	Maximum length: 35									
size	Maximum total size of files within the storage (MB).	integer	Minimum value: 16 Maximum value: 4294967295	16								
db-mode	Behavior when the maximum size is reached.	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.											
cache-mem-percent	Maximum percentage of available memory allocated to caching (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								

dnsfilter

This section includes syntax for the following commands:

- [config dnsfilter domain-filter on page 191](#)
- [config dnsfilter profile on page 192](#)

config dnsfilter domain-filter

Configure DNS domain filters.

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

config dnsfilter domain-filter

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

config entries

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

config dnsfilter profile

Configure DNS domain filter profile.

```
config dnsfilter profile
  Description: Configure DNS domain filter profile.
  edit <name>
    set comment {var-string}
    config domain-filter
      Description: Domain filter settings.
      set domain-filter-table {integer}
    end
```

```

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

```

config dnsfilter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default								
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging of all domains visited.</td></tr><tr><td><i>disable</i></td><td>Disable logging of all domains visited.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of all domains visited.	<i>disable</i>	Disable logging of all domains visited.					
Option	Description											
<i>enable</i>	Enable logging of all domains visited.											
<i>disable</i>	Disable logging of all domains visited.											
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard SDNS rating error logging.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard SDNS rating error logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard SDNS rating error logging.	<i>disable</i>	Disable FortiGuard SDNS rating error logging.					
Option	Description											
<i>enable</i>	Enable FortiGuard SDNS rating error logging.											
<i>disable</i>	Disable FortiGuard SDNS rating error logging.											
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable domain filtering and botnet domain logging.</td></tr><tr><td><i>disable</i></td><td>Disable domain filtering and botnet domain logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable domain filtering and botnet domain logging.	<i>disable</i>	Disable domain filtering and botnet domain logging.					
Option	Description											
<i>enable</i>	Enable domain filtering and botnet domain logging.											
<i>disable</i>	Disable domain filtering and botnet domain logging.											
block-action	Action to take for blocked domains.	option	-	redirect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Return NXDOMAIN for blocked domains.</td></tr><tr><td><i>redirect</i></td><td>Redirect blocked domains to SDNS portal.</td></tr><tr><td><i>block-sevrfail</i></td><td>Return SERVFAIL for blocked domains.</td></tr></table>	Option	Description	<i>block</i>	Return NXDOMAIN for blocked domains.	<i>redirect</i>	Redirect blocked domains to SDNS portal.	<i>block-sevrfail</i>	Return SERVFAIL for blocked domains.			
Option	Description											
<i>block</i>	Return NXDOMAIN for blocked domains.											
<i>redirect</i>	Redirect blocked domains to SDNS portal.											
<i>block-sevrfail</i>	Return SERVFAIL for blocked domains.											
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	::								
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable blocking botnet C&C DNS lookups.</td></tr><tr><td><i>enable</i></td><td>Enable blocking botnet C&C DNS lookups.</td></tr></table>	Option	Description	<i>disable</i>	Disable blocking botnet C&C DNS lookups.	<i>enable</i>	Enable blocking botnet C&C DNS lookups.					
Option	Description											
<i>disable</i>	Disable blocking botnet C&C DNS lookups.											
<i>enable</i>	Enable blocking botnet C&C DNS lookups.											

Parameter	Description	Type	Size	Default								
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td></tr><tr><td><i>enable</i></td><td>Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td></tr></table>	Option	Description	<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.					
Option	Description											
<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.											
<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.											
youtube-restrict	Set safe search for YouTube restriction level.	option	-	strict								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Enable strict safe seach for YouTube.</td></tr><tr><td><i>moderate</i></td><td>Enable moderate safe search for YouTube.</td></tr><tr><td><i>none</i></td><td>Disable safe search for YouTube.</td></tr></table>	Option	Description	<i>strict</i>	Enable strict safe seach for YouTube.	<i>moderate</i>	Enable moderate safe search for YouTube.	<i>none</i>	Disable safe search for YouTube.			
Option	Description											
<i>strict</i>	Enable strict safe seach for YouTube.											
<i>moderate</i>	Enable moderate safe search for YouTube.											
<i>none</i>	Disable safe search for YouTube.											
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79									
transparent-dns-database <name>	Transparent DNS database zones. DNS database zone name.	string	Maximum length: 79									
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><i>disable</i></td><td>Disable removal of the encrypted client hello service parameter from supporting DNS RRs.</td></tr><tr><td><i>enable</i></td><td>Enable removal of the encrypted client hello service parameter from supporting DNS RRs.</td></tr></table>	Option	Description	<i>disable</i>	Disable removal of the encrypted client hello service parameter from supporting DNS RRs.	<i>enable</i>	Enable removal of the encrypted client hello service parameter from supporting DNS RRs.					
Option	Description											
<i>disable</i>	Disable removal of the encrypted client hello service parameter from supporting DNS RRs.											
<i>enable</i>	Enable removal of the encrypted client hello service parameter from supporting DNS RRs.											

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
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
category	Category number.	integer	Minimum value: 0 Maximum value: 255	0
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.		
log	Enable/disable DNS filter logging for this DNS profile.	option	-	enable
	Option Description			
	<i>enable</i>	Enable DNS filter logging.		
	<i>disable</i>	Disable DNS filter logging.		

config dns-translation

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
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						
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						
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						
status	Enable/disable this DNS translation entry.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this DNS translation.</td></tr><tr><td>disable</td><td>Disable this DNS translation.</td></tr></table>				Option	Description	enable	Enable this DNS translation.	disable	Disable this DNS translation.
	Option	Description								
	enable	Enable this DNS translation.								
disable	Disable this DNS translation.									

Parameter	Description	Type	Size	Default
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	::
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	::
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 Maximum value: 128	128

emailfilter

This section includes syntax for the following commands:

- [config emailfilter block-allow-list on page 199](#)
- [config emailfilter bword on page 201](#)
- [config emailfilter dnsbl on page 203](#)
- [config emailfilter fortishield on page 205](#)
- [config emailfilter iptrust on page 205](#)
- [config emailfilter mheader on page 207](#)
- [config emailfilter options on page 208](#)
- [config emailfilter profile on page 209](#)

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

config emailfilter block-allow-list

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

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.		
action	Reject, mark as spam or good email.	option	-	spam
	Option	Description		
	<i>reject</i>	Reject the connection.		
	<i>spam</i>	Mark as spam email.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>clear</i>	Mark as good email.		
addr-type	IP address type.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 Address type.		
	<i>ipv6</i>	IPv6 Address type.		
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-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regex</i>	Perl regular expression.		
pattern	Pattern to match.	string	Maximum length: 127	

config emailfilter bword

Configure AntiSpam banned word list.

```

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

```

```
next
end
```

config emailfilter bword

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

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	Banned word entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
pattern	Pattern for the banned word.	string	Maximum length: 127	
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regex</i>	Perl regular expression.		
action	Mark spam or good.	option	-	spam

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>spam</i>	Mark as spam email.		
	<i>clear</i>	Mark as good email.		
where	Component of the email to be scanned.	option	-	all
	Option	Description		
	<i>subject</i>	Banned word in email subject.		
	<i>body</i>	Banned word in email body.		
	<i>all</i>	Banned word in both subject and body.		
language	Language for the 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.		
score	Score value.	integer	Minimum value: 1 Maximum value: 99999	10

config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

```
config emailfilter dnsbl
  Description: Configure AntiSpam DNSBL/ORBL.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter DNSBL and ORBL server.
      edit <id>
```

```

        set status [enable|disable]
        set server {string}
        set action [reject|spam]
    next
end
next
end

```

config emailfilter dnsbl

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

config entries

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

config emailfilter fortishield

Configure FortiGuard - AntiSpam.

```
config emailfilter fortishield
  Description: Configure FortiGuard - AntiSpam.
  set spam-submit-srv {string}
  set spam-submit-force [enable|disable]
  set spam-submit-txt2htm [enable|disable]
end
```

config emailfilter fortishield

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

config emailfilter iptrust

Configure AntiSpam IP trust.

```
config emailfilter iptrust
  Description: Configure AntiSpam IP trust.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter trusted IP addresses.
```

```

edit <id>
    set status [enable|disable]
    set addr-type [ipv4|ipv6]
    set ip4-subnet {ipv4-classnet}
    set ip6-subnet {ipv6-network}
next
end
next
end

```

config emailfilter iptrust

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

config entries

Parameter	Description	Type	Size	Default						
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.									
id	Trusted IP entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
addr-type	Type of address.	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.									

Parameter	Description	Type	Size	Default
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

config emailfilter mheader

Configure AntiSpam MIME header.

```

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

```

config emailfilter mheader

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

config entries

Parameter	Description	Type	Size	Default						
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.									
id	Mime header entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
fieldname	Pattern for header field name.	string	Maximum length: 63							
fieldbody	Pattern for the header field body.	string	Maximum length: 127							
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wildcard</i></td><td>Wildcard pattern.</td></tr><tr><td><i>regex</i></td><td>Perl regular expression.</td></tr></table>	Option	Description	<i>wildcard</i>	Wildcard pattern.	<i>regex</i>	Perl regular expression.			
Option	Description									
<i>wildcard</i>	Wildcard pattern.									
<i>regex</i>	Perl regular expression.									
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.									

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 replacemsg-group {string}
    set spam-log [disable|enable]
    set spam-log-fortiguard-response [disable|enable]
    set spam-filtering [enable|disable]
    set external [enable|disable]
    set options {option1}, {option2}, ...
    config imap
      Description: IMAP.
      set log-all [disable|enable]
      set action [pass|tag]
      set tag-type {option1}, {option2}, ...
      set tag-msg {string}
    end
    config pop3
      Description: POP3.
      set log-all [disable|enable]
      set action [pass|tag]
      set tag-type {option1}, {option2}, ...
      set tag-msg {string}
    end
    config smtp
      Description: SMTP.
      set log-all [disable|enable]
      set action [pass|tag|...]
      set tag-type {option1}, {option2}, ...
      set tag-msg {string}
      set hdrrip [disable|enable]
      set local-override [disable|enable]
    end
    config mapi
      Description: MAPI.
      set log-all [disable|enable]
```

```

        set action [pass|discard]
    end
    config msn-hotmail
        Description: MSN Hotmail.
        set log-all [disable|enable]
    end
    config yahoo-mail
        Description: Yahoo! Mail.
        set log-all [disable|enable]
    end
    config gmail
        Description: Gmail.
        set log-all [disable|enable]
    end
    config other-webmails
        Description: Other supported webmails.
        set log-all [disable|enable]
    end
    set spam-bword-threshold {integer}
    set spam-bword-table {integer}
    set spam-bal-table {integer}
    set spam-mheader-table {integer}
    set spam-rbl-table {integer}
    set spam-iptrust-table {integer}
next
end

```

config emailfilter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
spam-log	Enable/disable spam logging for email filtering.	option	-	enable
		Option	Description	
		<i>disable</i>	Disable spam logging for email filtering.	
		<i>enable</i>	Enable spam logging for email filtering.	

Parameter	Description	Type	Size	Default																								
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging FortiGuard spam response.</td></tr><tr><td>enable</td><td>Enable logging FortiGuard spam response.</td></tr></table>	Option	Description	disable	Disable logging FortiGuard spam response.	enable	Enable logging FortiGuard spam response.																					
	Option	Description																										
	disable	Disable logging FortiGuard spam response.																										
enable	Enable logging FortiGuard spam response.																											
spam-filtering	Enable/disable spam filtering.	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.																											
external	Enable/disable external Email inspection.	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.																											
options	Options.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bannedword</td><td>Content block.</td></tr><tr><td>spambal</td><td>Block/allow list.</td></tr><tr><td>spamfsip</td><td>Email IP address FortiGuard AntiSpam block list check.</td></tr><tr><td>spamfssubmit</td><td>Add FortiGuard AntiSpam spam submission text.</td></tr><tr><td>spamfschksum</td><td>Email checksum FortiGuard AntiSpam check.</td></tr><tr><td>spamfsurl</td><td>Email content URL FortiGuard AntiSpam check.</td></tr><tr><td>spamhelodns</td><td>Email helo/ehlo domain DNS check.</td></tr><tr><td>spamraddrdns</td><td>Email return address DNS check.</td></tr><tr><td>spamrbl</td><td>Email DNSBL & ORBL check.</td></tr><tr><td>spamhdrcheck</td><td>Email mime header check.</td></tr><tr><td>spamfsphish</td><td>Email content phishing URL FortiGuard AntiSpam check.</td></tr></table>	Option	Description	bannedword	Content block.	spambal	Block/allow list.	spamfsip	Email IP address FortiGuard AntiSpam block list check.	spamfssubmit	Add FortiGuard AntiSpam spam submission text.	spamfschksum	Email checksum FortiGuard AntiSpam check.	spamfsurl	Email content URL FortiGuard AntiSpam check.	spamhelodns	Email helo/ehlo domain DNS check.	spamraddrdns	Email return address DNS check.	spamrbl	Email DNSBL & ORBL check.	spamhdrcheck	Email mime header check.	spamfsphish	Email content phishing URL FortiGuard AntiSpam check.			
	Option	Description																										
	bannedword	Content block.																										
	spambal	Block/allow list.																										
	spamfsip	Email IP address FortiGuard AntiSpam block list check.																										
	spamfssubmit	Add FortiGuard AntiSpam spam submission text.																										
	spamfschksum	Email checksum FortiGuard AntiSpam check.																										
	spamfsurl	Email content URL FortiGuard AntiSpam check.																										
	spamhelodns	Email helo/ehlo domain DNS check.																										
	spamraddrdns	Email return address DNS check.																										
	spamrbl	Email DNSBL & ORBL check.																										
spamhdrcheck	Email mime header check.																											
spamfsphish	Email content phishing URL FortiGuard AntiSpam check.																											

Parameter	Description	Type	Size	Default
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-bal-table	Anti-spam block/allow list table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-mheader-table	Anti-spam MIME header table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-rbl-table	Anti-spam DNSBL table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config imap

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.		
action	Action for spam email.	option	-	tag

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>tag</i>	Tag spam email with configured text in subject or header.		
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.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

config pop3

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.		
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.		
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.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

config smtp

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

config mapi

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.		
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.		

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 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.		

config gmail

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 other-webmails

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 222](#)
- [config endpoint-control fctems on page 217](#)
- [config endpoint-control settings on page 227](#)

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 status [enable|disable]
    set name {string}
    set dirty-reason [none|mismatched-ems-sn]
    set fortinetone-cloud-authentication [enable|disable]
    set cloud-authentication-access-key {string}
    set server {string}
    set https-port {integer}
    set serial-number {string}
    set tenant-id {string}
    set source-ip {ipv4-address-any}
    set pull-sysinfo [enable|disable]
    set pull-vulnerabilities [enable|disable]
    set pull-avatars [enable|disable]
    set pull-tags [enable|disable]
    set pull-malware-hash [enable|disable]
    set capabilities {option1}, {option2}, ...
    set call-timeout {integer}
    set out-of-sync-threshold {integer}
    set send-tags-to-all-vdoms [enable|disable]
    set websocket-override [enable|disable]
    set preserve-ssl-session [enable|disable]
    set interface-select-method [auto|specify]
    set interface {string}
    set trust-ca-cn [enable|disable]
    set verifying-ca {string}
  next
end
```

config endpoint-control fctems

Parameter	Description	Type	Size	Default
ems-id	EMS ID in order (1 - 7).	integer	Minimum value: 1 Maximum value: 7	0
status	Enable or disable this EMS configuration.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable EMS configuration and operation.		
	<i>disable</i>	Disable EMS configuration and operation.		
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35	
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.		
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable authentication of FortiClient EMS Cloud through FortiCloud account.		
	<i>disable</i>	Disable authentication of FortiClient EMS Cloud through FortiCloud account.		
cloud-authentication-access-key	FortiClient EMS Cloud multitenancy access key	string	Maximum length: 20	
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255	
https-port	FortiClient EMS HTTPS access port number. (1 - 65535, default: 443).	integer	Minimum value: 1 Maximum value: 65535	443

Parameter	Description	Type	Size	Default						
serial-number	EMS Serial Number.	string	Maximum length: 16							
tenant-id	EMS Tenant ID.	string	Maximum length: 32							
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0						
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-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.									
pull-avatars	Enable/disable pulling avatars from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user avatars from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user avatars from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user avatars from EMS.	<i>disable</i>	Disable pulling FortiClient user avatars from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient user avatars from EMS.									
<i>disable</i>	Disable pulling FortiClient user avatars 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-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.									

Parameter	Description	Type	Size	Default																								
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 FortiProxy 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 FortiProxy HA clusters on EMS in the Security Fabric.</td></tr><tr><td><i>websocket</i></td><td>Enable/disable websockets for this FortiProxy 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 recieve 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 FortiProxy 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 FortiProxy HA clusters on EMS in the Security Fabric.	<i>websocket</i>	Enable/disable websockets for this FortiProxy 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 recieve 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 FortiProxy 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 FortiProxy HA clusters on EMS in the Security Fabric.																										
	<i>websocket</i>	Enable/disable websockets for this FortiProxy 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 recieve 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.																											
call-timeout	FortiClient EMS call timeout in seconds (1 - 180 seconds, default = 30).	integer	Minimum value: 1 Maximum value: 180	30																								
out-of-sync-threshold	Outdated resource threshold in seconds (10 - 3600, default = 180).	integer	Minimum value: 10 Maximum value: 3600	180																								
send-tags-to-all-vdoms	Relax restrictions on tags to send all EMS tags to all VDOMs	option	-	disable																								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sending tags to all vdoms.		
	<i>disable</i>	Disable sending tags to all vdoms.		
websocket-override	Enable/disable override behavior for how this FortiProxy unit connects to EMS using a WebSocket connection.	option	-	disable
	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.		
preserve-ssl-session	Enable/disable preservation of EMS SSL session connection. Warning, most users should not touch this setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Allow preservation of EMS SSL session connection.		
	<i>disable</i>	Don't allow preservation of EMS SSL session connection.		
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
trust-ca-cn	Enable/disable trust of the EMS certificate issuer(CA) and common name (CN) for certificate auto-renewal.	option	-	enable
	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.		

Parameter	Description	Type	Size	Default
verifying-ca	Lowest CA cert on Fortigate in verified EMS cert chain.	string	Maximum length: 79	

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 status [enable|disable]
        set name {string}
        set dirty-reason [none|mismatched-ems-sn]
        set fortinetone-cloud-authentication [enable|disable]
        set cloud-authentication-access-key {string}
        set server {string}
        set https-port {integer}
        set serial-number {string}
        set tenant-id {string}
        set source-ip {ipv4-address-any}
        set pull-sysinfo [enable|disable]
        set pull-vulnerabilities [enable|disable]
        set pull-avatars [enable|disable]
        set pull-tags [enable|disable]
        set pull-malware-hash [enable|disable]
        set capabilities {option1}, {option2}, ...
        set call-timeout {integer}
        set out-of-sync-threshold {integer}
        set send-tags-to-all-vdms [enable|disable]
        set websocket-override [enable|disable]
        set preserve-ssl-session [enable|disable]
        set interface-select-method [auto|specify]
        set interface {string}
        set trust-ca-cn [enable|disable]
        set verifying-ca {string}
    next
end

```

config endpoint-control fctems-override

Parameter	Description	Type	Size	Default
ems-id	EMS ID in order (1 - 7).	integer	Minimum value: 1 Maximum value: 7	0
status	Enable or disable this EMS configuration.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable EMS configuration and operation.		
	<i>disable</i>	Disable EMS configuration and operation.		
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35	
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.		
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable authentication of FortiClient EMS Cloud through FortiCloud account.		
	<i>disable</i>	Disable authentication of FortiClient EMS Cloud through FortiCloud account.		
cloud-authentication-access-key	FortiClient EMS Cloud multitenancy access key	string	Maximum length: 20	
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255	
https-port	FortiClient EMS HTTPS access port number. (1 - 65535, default: 443).	integer	Minimum value: 1 Maximum value: 65535	443

Parameter	Description	Type	Size	Default						
serial-number	EMS Serial Number.	string	Maximum length: 16							
tenant-id	EMS Tenant ID.	string	Maximum length: 32							
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0						
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-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.									
pull-avatars	Enable/disable pulling avatars from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user avatars from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user avatars from EMS.</td></tr></table>				Option	Description	<i>enable</i>	Enable pulling FortiClient user avatars from EMS.	<i>disable</i>	Disable pulling FortiClient user avatars from EMS.
Option	Description									
<i>enable</i>	Enable pulling FortiClient user avatars from EMS.									
<i>disable</i>	Disable pulling FortiClient user avatars 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-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.									

Parameter	Description	Type	Size	Default
capabilities	List of EMS capabilities.	option	-	
	Option	Description		
	<i>fabric-auth</i>	Allow this FortiProxy 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 FortiProxy HA clusters on EMS in the Security Fabric.		
	<i>websocket</i>	Enable/disable websockets for this FortiProxy 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 recieve 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.			
call-timeout	FortiClient EMS call timeout in seconds (1 - 180 seconds, default = 30).	integer	Minimum value: 1 Maximum value: 180	30
out-of-sync-threshold	Outdated resource threshold in seconds (10 - 3600, default = 180).	integer	Minimum value: 10 Maximum value: 3600	180
send-tags-to-all-vdoms	Relax restrictions on tags to send all EMS tags to all VDOMs	option	-	disable

Parameter	Description	Type	Size	Default						
	<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.									
websocket-override	Enable/disable override behavior for how this FortiProxy 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.									
preserve-ssl-session	Enable/disable preservation of EMS SSL session connection. Warning, most users should not touch this setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow preservation of EMS SSL session connection.</td></tr><tr><td><i>disable</i></td><td>Don't allow preservation of EMS SSL session connection.</td></tr></table>	Option	Description	<i>enable</i>	Allow preservation of EMS SSL session connection.	<i>disable</i>	Don't allow preservation of EMS SSL session connection.			
	Option	Description								
	<i>enable</i>	Allow preservation of EMS SSL session connection.								
<i>disable</i>	Don't allow preservation of EMS SSL session connection.									
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
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.									

Parameter	Description	Type	Size	Default
verifying-ca	Lowest CA cert on Fortigate in verified EMS cert chain.	string	Maximum length: 79	

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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Overriding global EMS table.</td></tr><tr><td><i>disable</i></td><td>Disable Overriding global EMS table.</td></tr></table>				Option	Description	<i>enable</i>	Enable Overriding global EMS table.	<i>disable</i>	Disable Overriding global EMS table.
Option	Description									
<i>enable</i>	Enable Overriding global EMS table.									
<i>disable</i>	Disable Overriding global EMS table.									

file-filter

This section includes syntax for the following commands:

- [config file-filter profile on page 228](#)

config file-filter profile

Configure file-filter profiles.

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

config file-filter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
log	Enable/disable file-filter logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
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
name	File-filter rule name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
protocol	Protocols to apply rule to.	option	-	http ftp smtp imap pop3 mapi cifs ssh
	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.)		
action	Action taken for matched file.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Allow the content and write a log message.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the content and write a log message.		
direction	Traffic direction (HTTP, FTP, SSH, CIFS, and MAPI only).	option	-	any
	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.		
password-protected	Match password-protected files.	option	-	any
	Option	Description		
	<i>yes</i>	Match only password-protected files.		
	<i>any</i>	Match any file.		
file-type <name>	Select file type. File type name.	string	Maximum length: 39	

firewall

This section includes syntax for the following commands:

- [config firewall access-proxy-ssh-client-cert on page 306](#)
- [config firewall access-proxy-virtual-host on page 308](#)
- [config firewall access-proxy on page 232](#)
- [config firewall access-proxy6 on page 269](#)
- [config firewall address on page 309](#)
- [config firewall address6 on page 315](#)
- [config firewall addrgrp on page 319](#)
- [config firewall addrgrp6 on page 322](#)
- [config firewall auth-portal on page 323](#)
- [config firewall central-snat-map on page 324](#)
- [config firewall city on page 326](#)
- [config firewall country on page 326](#)
- [config firewall decrypted-traffic-mirror on page 327](#)
- [config firewall global on page 328](#)
- [config firewall identity-based-route on page 329](#)
- [config firewall internet-service-addition on page 332](#)
- [config firewall internet-service-append on page 333](#)
- [config firewall internet-service-botnet on page 334](#)
- [config firewall internet-service-custom-group on page 337](#)
- [config firewall internet-service-custom on page 335](#)
- [config firewall internet-service-definition on page 337](#)
- [config firewall internet-service-extension on page 339](#)
- [config firewall internet-service-group on page 343](#)
- [config firewall internet-service-ipbl-reason on page 344](#)
- [config firewall internet-service-ipbl-vendor on page 344](#)
- [config firewall internet-service-list on page 345](#)
- [config firewall internet-service-name on page 345](#)
- [config firewall internet-service-owner on page 346](#)
- [config firewall internet-service-reputation on page 347](#)
- [config firewall internet-service-sld on page 348](#)
- [config firewall internet-service-subapp on page 348](#)
- [config firewall internet-service on page 330](#)
- [config firewall ippool on page 349](#)
- [config firewall ippool6 on page 349](#)
- [config firewall network-service-dynamic on page 350](#)
- [config firewall on-demand-sniffer on page 351](#)

-
- [config firewall policy on page 353](#)
 - [config firewall profile-group on page 366](#)
 - [config firewall profile-protocol-options on page 368](#)
 - [config firewall proxy-address on page 393](#)
 - [config firewall proxy-address6 on page 398](#)
 - [config firewall proxy-addrgrp on page 402](#)
 - [config firewall proxy-addrgrp6 on page 404](#)
 - [config firewall region on page 405](#)
 - [config firewall response-shaping-policy on page 406](#)
 - [config firewall schedule group on page 408](#)
 - [config firewall schedule onetime on page 409](#)
 - [config firewall schedule recurring on page 410](#)
 - [config firewall service category on page 411](#)
 - [config firewall service custom on page 412](#)
 - [config firewall service group on page 416](#)
 - [config firewall shaper per-ip-shaper on page 417](#)
 - [config firewall shaper traffic-shaper on page 418](#)
 - [config firewall shaping-policy on page 421](#)
 - [config firewall shaping-profile on page 425](#)
 - [config firewall sniffer on page 426](#)
 - [config firewall ssh host-key on page 428](#)
 - [config firewall ssh local-ca on page 430](#)
 - [config firewall ssh local-key on page 430](#)
 - [config firewall ssh setting on page 431](#)
 - [config firewall ssl-server on page 435](#)
 - [config firewall ssl-ssh-profile on page 438](#)
 - [config firewall ssl default-certificate on page 432](#)
 - [config firewall ssl keyring-list on page 433](#)
 - [config firewall ssl setting on page 433](#)
 - [config firewall traffic-class on page 471](#)
 - [config firewall ttl-policy on page 471](#)
 - [config firewall vendor-mac-summary on page 473](#)
 - [config firewall vendor-mac on page 472](#)
 - [config firewall vip on page 473](#)
 - [config firewall vipgrp on page 509](#)
 - [config firewall wildcard-fqdn custom on page 510](#)
 - [config firewall wildcard-fqdn group on page 511](#)

config firewall access-proxy

Configure IPv4 access proxy.

```

config firewall access-proxy
    Description: Configure IPv4 access proxy.
    edit <name>
        set vip {string}
        set auth-portal [disable|enable]
        set auth-virtual-host {string}
        set log-blocked-traffic [enable|disable]
        set add-vhost-domain-to-dnsdb [enable|disable]
        set svr-pool-multiplex [enable|disable]
        set svr-pool-ttl {integer}
        set svr-pool-server-max-request {integer}
        set svr-pool-server-max-concurrent-request {integer}
        set decrypted-traffic-mirror {string}
    config api-gateway
        Description: Set IPv4 API Gateway.
        edit <id>
            set url-map {string}
            set service [http|https|...]
            set ldb-method [static|round-robin|...]
            set virtual-host {string}
            set url-map-type [sub-string|wildcard|...]
            set h2-support [enable|disable]
            set h3-support [enable|disable]
        config quic
            Description: QUIC setting.
            set max-idle-timeout {integer}
            set max-udp-payload-size {integer}
            set active-connection-id-limit {integer}
            set ack-delay-exponent {integer}
            set max-ack-delay {integer}
            set max-datagram-frame-size {integer}
            set active-migration [enable|disable]
            set grease-quic-bit [enable|disable]
        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 ip {ipv4-address-any}
            set domain {string}
            set port {integer}
            set mappedport {user}
            set status [active|standby|...]
            set type [tcp-forwarding|ssh]
            set external-auth [enable|disable]
            set tunnel-encryption [enable|disable]
            set weight {integer}
            set http-host {string}
            set health-check [disable|enable]
            set health-check-proto [ping|http|...]

```

```

        set holddown-interval [enable|disable]
        set translate-host [enable|disable]
        set ssh-client-cert {string}
        set ssh-host-key-validation [disable|enable]
        set ssh-host-key <name1>, <name2>, ...
        set verify-cert [enable|disable]
    next
end
set application <name1>, <name2>, ...
set persistence [none|http-cookie]
set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set saml-server {string}
set saml-redirect [disable|enable]
set ssl-dh-bits [768|1024|...]
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-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https|...]
        set ldb-method [static|round-robin|...]
        set virtual-host {string}
        set url-map-type [sub-string|wildcard|...]
        set h2-support [enable|disable]
        set h3-support [enable|disable]
    config quic
        Description: QUIC setting.
        set max-idle-timeout {integer}
        set max-udp-payload-size {integer}
        set active-connection-id-limit {integer}
        set ack-delay-exponent {integer}
        set max-ack-delay {integer}
        set max-datagram-frame-size {integer}
        set active-migration [enable|disable]
    
```

```

        set grease-quic-bit [enable|disable]
    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 ip {ipv6-address}
            set domain {string}
            set port {integer}
            set mappedport {user}
            set status [active|standby|...]
            set type [tcp-forwarding|ssh]
            set external-auth [enable|disable]
            set tunnel-encryption [enable|disable]
            set weight {integer}
            set http-host {string}
            set health-check [disable|enable]
            set health-check-proto [ping|http|...]
            set holddown-interval [enable|disable]
            set translate-host [enable|disable]
            set ssh-client-cert {string}
            set ssh-host-key-validation [disable|enable]
            set ssh-host-key <name1>, <name2>, ...
            set verify-cert [enable|disable]
        next
    end
    set application <name1>, <name2>, ...
    set persistence [none|http-cookie]
    set http-cookie-domain-from-host [disable|enable]
    set http-cookie-domain {string}
    set http-cookie-path {string}
    set http-cookie-generation {integer}
    set http-cookie-age {integer}
    set http-cookie-share [disable|same-ip]
    set https-cookie-secure [disable|enable]
    set saml-server {string}
    set saml-redirect [disable|enable]
    set ssl-dh-bits [768|1024|...]
    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-min-version [tls-1.0|tls-1.1|...]
    set ssl-max-version [tls-1.0|tls-1.1|...]
    set ssl-renegotiation [enable|disable]
next

```

```
end
next
end
```

config firewall access-proxy

Parameter	Description	Type	Size	Default						
name	Access Proxy name.	string	Maximum length: 79							
vip	Virtual IP name.	string	Maximum length: 79							
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication portal.</td></tr><tr><td><i>enable</i></td><td>Enable authentication portal.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication portal.	<i>enable</i>	Enable authentication portal.			
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							
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log all traffic denied by this access proxy.</td></tr><tr><td><i>disable</i></td><td>Do not log all traffic denied by this access proxy.</td></tr></table>	Option	Description	<i>enable</i>	Log all traffic denied by this access proxy.	<i>disable</i>	Do not log all traffic denied by this access proxy.			
Option	Description									
<i>enable</i>	Log all traffic denied by this access proxy.									
<i>disable</i>	Do not log all traffic denied by this access proxy.									
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><i>enable</i></td><td>add dns entry for all vhosts used by access proxy.</td></tr><tr><td><i>disable</i></td><td>Do not add dns entry for all vhosts used by access proxy.</td></tr></table>	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.			
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.									
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><i>enable</i></td><td>Enable server pool multiplexing. Share connected server.</td></tr><tr><td><i>disable</i></td><td>Disable server pool multiplexing. Do not share connected server.</td></tr></table>	Option	Description	<i>enable</i>	Enable server pool multiplexing. Share connected server.	<i>disable</i>	Disable server pool multiplexing. Do not share connected server.			
Option	Description									
<i>enable</i>	Enable server pool multiplexing. Share connected server.									
<i>disable</i>	Disable server pool multiplexing. Do not share connected server.									

Parameter	Description	Type	Size	Default
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15
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-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
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	

config api-gateway

Parameter	Description	Type	Size	Default
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option Description			
	http HTTP.			
	https HTTPS.			
	tcp-forwarding TCP-FORWARDING.			
	samlsp SAML-SP.			
	saas SAAS.			
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.															
virtual-host	Virtual host.	string	Maximum length: 79													
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.															
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.															
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79													
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												

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>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.									
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><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	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.			
	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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
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-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-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><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						

Parameter	Description	Type	Size	Default
	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.		
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not support redirection after successful SAML authentication.		
	<i>enable</i>	Support redirection after successful SAML authentication.		
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	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.		
	<i>3072</i>	3072-bit Diffie-Hellman prime.		
	<i>4096</i>	4096-bit Diffie-Hellman prime.		
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	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-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1

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-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-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.													

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
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						
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.									

config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
	Option	Description		
	ip	Standard IPv4 address.		
	fqdn	Non-wildcard FQDN address object.		

Parameter	Description	Type	Size	Default								
address	Address or address group of the real server.	string	Maximum length: 79									
ip	IP address of the real server.	ipv4-address-any	Not Specified	0.0.0.0								
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
mappedport	Port for communicating with the real server.	user	Not Specified									
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.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp-forwarding</td><td>TCP forwarding.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>				Option	Description	tcp-forwarding	TCP forwarding.	ssh	SSH.		
Option	Description											
tcp-forwarding	TCP forwarding.											
ssh	SSH.											
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.											

Parameter	Description	Type	Size	Default								
tunnel-encryption	Tunnel encryption.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable tcp forwarding tunnel encryption.</td></tr><tr><td><i>disable</i></td><td>Disable tcp forwarding tunnel encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable tcp forwarding tunnel encryption.	<i>disable</i>	Disable tcp forwarding tunnel encryption.					
Option	Description											
<i>enable</i>	Enable tcp forwarding tunnel encryption.											
<i>disable</i>	Disable tcp forwarding tunnel encryption.											
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								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
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.											

Parameter	Description	Type	Size	Default						
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.									
ssh-client-cert	Set access-proxy SSH client certificate profile.	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.									
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79							
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.									

config ssl-cipher-suites

Parameter	Description	Type	Size	Default				
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0				
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></table>	Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.			
Option	Description							
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	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.		
	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.		

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></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-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.									
Option	Description													
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.													
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
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option Description			
	http	HTTP.		
	https	HTTPS.		
	tcp-forwarding	TCP-FORWARDING.		
	samlsp	SAML-SP.		
	saas	SAAS.		
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.															
virtual-host	Virtual host.	string	Maximum length: 79													
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.															
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.															
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79													
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												

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>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.									
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><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	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.			
	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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
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-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-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><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						

Parameter	Description	Type	Size	Default
	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.		
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not support redirection after successful SAML authentication.		
	<i>enable</i>	Support redirection after successful SAML authentication.		
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	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.		
	<i>3072</i>	3072-bit Diffie-Hellman prime.		
	<i>4096</i>	4096-bit Diffie-Hellman prime.		
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	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-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1

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-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-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.													

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2

Parameter	Description	Type	Size	Default						
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3						
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						
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.									

config realservers

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

Parameter	Description	Type	Size	Default								
address	Address or address group of the real server.	string	Maximum length: 79									
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::								
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
mappedport	Port for communicating with the real server.	user	Not Specified									
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.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp-forwarding</td><td>TCP forwarding.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>				Option	Description	tcp-forwarding	TCP forwarding.	ssh	SSH.		
Option	Description											
tcp-forwarding	TCP forwarding.											
ssh	SSH.											
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.											

Parameter	Description	Type	Size	Default								
tunnel-encryption	Tunnel encryption.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable tcp forwarding tunnel encryption.</td></tr><tr><td><i>disable</i></td><td>Disable tcp forwarding tunnel encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable tcp forwarding tunnel encryption.	<i>disable</i>	Disable tcp forwarding tunnel encryption.					
Option	Description											
<i>enable</i>	Enable tcp forwarding tunnel encryption.											
<i>disable</i>	Disable tcp forwarding tunnel encryption.											
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								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
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.											

Parameter	Description	Type	Size	Default						
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.									
ssh-client-cert	Set access-proxy SSH client certificate profile.	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.									
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79							
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.									

config ssl-cipher-suites

Parameter	Description	Type	Size	Default				
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0				
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></table>	Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.			
Option	Description							
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
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 vip {string}
    set auth-portal [disable|enable]
    set auth-virtual-host {string}
    set log-blocked-traffic [enable|disable]
    set add-vhost-domain-to-dnsdb [enable|disable]
    set svr-pool-multiplex [enable|disable]
    set svr-pool-ttl {integer}
    set svr-pool-server-max-request {integer}
    set svr-pool-server-max-concurrent-request {integer}
    set decrypted-traffic-mirror {string}
  config api-gateway
    Description: Set IPv4 API Gateway.
    edit <id>
      set url-map {string}
      set service [http|https|...]
      set ldb-method [static|round-robin|...]
      set virtual-host {string}
      set url-map-type [sub-string|wildcard|...]
      set h2-support [enable|disable]
      set h3-support [enable|disable]
    config quic
      Description: QUIC setting.
```

```

        set max-idle-timeout {integer}
        set max-udp-payload-size {integer}
        set active-connection-id-limit {integer}
        set ack-delay-exponent {integer}
        set max-ack-delay {integer}
        set max-datagram-frame-size {integer}
        set active-migration [enable|disable]
        set grease-quick-bit [enable|disable]
    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 ip {ipv4-address-any}
            set domain {string}
            set port {integer}
            set mappedport {user}
            set status [active|standby|...]
            set type [tcp-forwarding|ssh]
            set external-auth [enable|disable]
            set tunnel-encryption [enable|disable]
            set weight {integer}
            set http-host {string}
            set health-check [disable|enable]
            set health-check-protocol [ping|http|...]
            set holddown-interval [enable|disable]
            set translate-host [enable|disable]
            set ssh-client-cert {string}
            set ssh-host-key-validation [disable|enable]
            set ssh-host-key <name1>, <name2>, ...
            set verify-cert [enable|disable]
        next
    end
    set application <name1>, <name2>, ...
    set persistence [none|http-cookie]
    set http-cookie-domain-from-host [disable|enable]
    set http-cookie-domain {string}
    set http-cookie-path {string}
    set http-cookie-generation {integer}
    set http-cookie-age {integer}
    set http-cookie-share [disable|same-ip]
    set https-cookie-secure [disable|enable]
    set saml-server {string}
    set saml-redirect [disable|enable]
    set ssl-dh-bits [768|1024|...]
    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-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https|...]
        set ldb-method [static|round-robin|...]
        set virtual-host {string}
        set url-map-type [sub-string|wildcard|...]
        set h2-support [enable|disable]
        set h3-support [enable|disable]
        config quic
            Description: QUIC setting.
            set max-idle-timeout {integer}
            set max-udp-payload-size {integer}
            set active-connection-id-limit {integer}
            set ack-delay-exponent {integer}
            set max-ack-delay {integer}
            set max-datagram-frame-size {integer}
            set active-migration [enable|disable]
            set grease-quic-bit [enable|disable]
        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 ip {ipv6-address}
                set domain {string}
                set port {integer}
                set mappedport {user}
                set status [active|standby|...]
                set type [tcp-forwarding|ssh]
                set external-auth [enable|disable]
                set tunnel-encryption [enable|disable]
                set weight {integer}
                set http-host {string}
                set health-check [disable|enable]
                set health-check-proto [ping|http|...]
                set holddown-interval [enable|disable]
                set translate-host [enable|disable]
                set ssh-client-cert {string}
                set ssh-host-key-validation [disable|enable]
                set ssh-host-key <name1>, <name2>, ...
            end
        end
    end
end

```

```

        set verify-cert [enable|disable]
    next
end
set application <name1>, <name2>, ...
set persistence [none|http-cookie]
set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set saml-server {string}
set saml-redirect [disable|enable]
set ssl-dh-bits [768|1024|...]
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-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
next
end
next
end

```

config firewall access-proxy6

Parameter	Description	Type	Size	Default						
name	Access Proxy name.	string	Maximum length: 79							
vip	Virtual IP name.	string	Maximum length: 79							
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication portal.</td></tr><tr><td><i>enable</i></td><td>Enable authentication portal.</td></tr></table>				Option	Description	<i>disable</i>	Disable authentication portal.	<i>enable</i>	Enable authentication portal.
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						
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.									
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.									
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.									
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15						
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-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						
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							

config api-gateway

Parameter	Description	Type	Size	Default												
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
url-map	URL pattern to match.	string	Maximum length: 511	/												
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>https</td><td>HTTPS.</td></tr><tr><td>tcp-forwarding</td><td>TCP-FORWARDING.</td></tr><tr><td>samlsp</td><td>SAML-SP.</td></tr><tr><td>saas</td><td>SAAS.</td></tr></table>	Option	Description	http	HTTP.	https	HTTPS.	tcp-forwarding	TCP-FORWARDING.	samlsp	SAML-SP.	saas	SAAS.			
Option	Description															
http	HTTP.															
https	HTTPS.															
tcp-forwarding	TCP-FORWARDING.															
samlsp	SAML-SP.															
saas	SAAS.															
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Distribute to server based on source IP.</td></tr><tr><td>round-robin</td><td>Distribute to server based round robin order.</td></tr><tr><td>weighted</td><td>Distribute to server based on weight.</td></tr><tr><td>first-alive</td><td>Distribute to the first server that is alive.</td></tr><tr><td>http-host</td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	static	Distribute to server based on source IP.	round-robin	Distribute to server based round robin order.	weighted	Distribute to server based on weight.	first-alive	Distribute to the first server that is alive.	http-host	Distribute to server based on host field in HTTP header.			
Option	Description															
static	Distribute to server based on source IP.															
round-robin	Distribute to server based round robin order.															
weighted	Distribute to server based on weight.															
first-alive	Distribute to the first server that is alive.															
http-host	Distribute to server based on host field in HTTP header.															
virtual-host	Virtual host.	string	Maximum length: 79													
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.															

Parameter	Description	Type	Size	Default						
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.									
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79							
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>none</td><td>None.</td></tr><tr><td>http-cookie</td><td>HTTP cookie.</td></tr></table>	Option	Description	none	None.	http-cookie	HTTP cookie.			
	Option	Description								
	none	None.								
http-cookie	HTTP cookie.									
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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
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-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-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.	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable
	Option		Description	
	<i>disable</i>		Do not support redirection after successful SAML authentication.	
	<i>enable</i>		Support redirection after successful SAML authentication.	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048

Parameter	Description	Type	Size	Default														
	<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-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>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.																	
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-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-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.		

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3
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
active-migration	Enable/disable active migration (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable active migration.		
	<i>disable</i>	Disable active migration.		

Parameter	Description	Type	Size	Default
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.		

config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
	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	
ip	IP address of the real server.	ipv4-address-any	Not Specified	0.0.0.0
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	
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.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-forwarding</i></td><td>TCP forwarding.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>tcp-forwarding</i>	TCP forwarding.	<i>ssh</i>	SSH.					
	Option	Description										
	<i>tcp-forwarding</i>	TCP forwarding.										
<i>ssh</i>	SSH.											
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><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.											
tunnel-encryption	Tunnel encryption.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable tcp forwarding tunnel encryption.</td></tr><tr><td><i>disable</i></td><td>Disable tcp forwarding tunnel encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable tcp forwarding tunnel encryption.	<i>disable</i>	Disable tcp forwarding tunnel encryption.					
	Option	Description										
	<i>enable</i>	Enable tcp forwarding tunnel encryption.										
<i>disable</i>	Disable tcp forwarding tunnel encryption.											
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								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								

Parameter	Description	Type	Size	Default
	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
	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
	Option	Description		
	<i>enable</i>	Enable per server holddown.		
	<i>disable</i>	Disable per server holddown.		
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable virtual hostname/IP translation.		
	<i>disable</i>	Disable virtual hostname/IP translation.		
ssh-client-cert	Set access-proxy SSH client certificate profile.	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.		
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

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.		

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.			

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></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-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-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																				
	<table><tr><th>Option</th><th>Description</th></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><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></table>	Option	Description	<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.	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.			
Option	Description																							
<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.																							
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																							

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></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><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></table>	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.			
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.																							
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												
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
url-map	URL pattern to match.	string	Maximum length: 511	/												
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>https</td><td>HTTPS.</td></tr><tr><td>tcp-forwarding</td><td>TCP-FORWARDING.</td></tr><tr><td>samlsp</td><td>SAML-SP.</td></tr><tr><td>saas</td><td>SAAS.</td></tr></table>				Option	Description	http	HTTP.	https	HTTPS.	tcp-forwarding	TCP-FORWARDING.	samlsp	SAML-SP.	saas	SAAS.
	Option	Description														
	http	HTTP.														
	https	HTTPS.														
	tcp-forwarding	TCP-FORWARDING.														
	samlsp	SAML-SP.														
	saas	SAAS.														
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Distribute to server based on source IP.</td></tr><tr><td>round-robin</td><td>Distribute to server based round robin order.</td></tr><tr><td>weighted</td><td>Distribute to server based on weight.</td></tr><tr><td>first-alive</td><td>Distribute to the first server that is alive.</td></tr><tr><td>http-host</td><td>Distribute to server based on host field in HTTP header.</td></tr></table>				Option	Description	static	Distribute to server based on source IP.	round-robin	Distribute to server based round robin order.	weighted	Distribute to server based on weight.	first-alive	Distribute to the first server that is alive.	http-host	Distribute to server based on host field in HTTP header.
	Option	Description														
	static	Distribute to server based on source IP.														
	round-robin	Distribute to server based round robin order.														
	weighted	Distribute to server based on weight.														
	first-alive	Distribute to the first server that is alive.														
http-host	Distribute to server based on host field in HTTP header.															
virtual-host	Virtual host.	string	Maximum length: 79													
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.															

Parameter	Description	Type	Size	Default						
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.									
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79							
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>none</td><td>None.</td></tr><tr><td>http-cookie</td><td>HTTP cookie.</td></tr></table>	Option	Description	none	None.	http-cookie	HTTP cookie.			
	Option	Description								
	none	None.								
http-cookie	HTTP cookie.									
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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
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-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-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.	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	enable
	Option		Description	
	<i>disable</i>		Do not support redirection after successful SAML authentication.	
	<i>enable</i>		Support redirection after successful SAML authentication.	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048

Parameter	Description	Type	Size	Default														
	<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-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>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.																	
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-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-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.		

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3
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
active-migration	Enable/disable active migration (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable active migration.		
	<i>disable</i>	Disable active migration.		

Parameter	Description	Type	Size	Default
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.		

config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
	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	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	
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.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-forwarding</i></td><td>TCP forwarding.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>tcp-forwarding</i>	TCP forwarding.	<i>ssh</i>	SSH.					
	Option	Description										
	<i>tcp-forwarding</i>	TCP forwarding.										
<i>ssh</i>	SSH.											
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><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.											
tunnel-encryption	Tunnel encryption.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable tcp forwarding tunnel encryption.</td></tr><tr><td><i>disable</i></td><td>Disable tcp forwarding tunnel encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable tcp forwarding tunnel encryption.	<i>disable</i>	Disable tcp forwarding tunnel encryption.					
	Option	Description										
	<i>enable</i>	Enable tcp forwarding tunnel encryption.										
<i>disable</i>	Disable tcp forwarding tunnel encryption.											
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								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								

Parameter	Description	Type	Size	Default
	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
	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
	Option	Description		
	<i>enable</i>	Enable per server holddown.		
	<i>disable</i>	Disable per server holddown.		
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable virtual hostname/IP translation.		
	<i>disable</i>	Disable virtual hostname/IP translation.		
ssh-client-cert	Set access-proxy SSH client certificate profile.	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.		
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

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.		

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.			

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		

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

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></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><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></table>	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.			
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
	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.		
versions	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
	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 source-address [enable|disable]
    set permit-x11-forwarding [enable|disable]
    set permit-agent-forwarding [enable|disable]
    set permit-port-forwarding [enable|disable]
    set permit-pty [enable|disable]
    set permit-user-rc [enable|disable]
    config cert-extension
      Description: Configure certificate extension for user certificate.
      edit <name>
        set critical [no|yes]
        set type [fixed|user]
        set data {string}
      next
    end
    set auth-ca {string}
  next
end
```

config firewall access-proxy-ssh-client-cert

Parameter	Description	Type	Size	Default						
name	SSH client certificate name.	string	Maximum length: 79							
source-address	Enable/disable appending source-address certificate critical option. This option ensure certificate only accepted from FortiGate source address.	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.									
permit-x11-forwarding	Enable/disable appending permit-x11-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.									

Parameter	Description	Type	Size	Default						
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						
	<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-pty	Enable/disable appending permit-pty 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-user-rc	Enable/disable appending permit-user-rc 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.									
auth-ca	Name of the SSH server public key authentication CA.	string	Maximum length: 79							

config cert-extension

Parameter	Description	Type	Size	Default
name	Name of certificate extension.	string	Maximum length: 127	
critical	Critical option.	option	-	no

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

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 ssl-certificate <name1>, <name2>, ...
        set host {string}
        set host-type [sub-string|wildcard]
        set replacemsg-group {string}
        set empty-cert-action [accept|block|...]
        set user-agent-detect [disable|enable]
        set client-cert [disable|enable]
    next
end

```

config firewall access-proxy-virtual-host

Parameter	Description	Type	Size	Default
name	Virtual host name.	string	Maximum length: 79	
ssl-certificate <name>	SSL certificates for this host. Certificate list.	string	Maximum length: 79	

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

config firewall address

Configure IPv4 addresses.

```

config firewall address
    Description: Configure IPv4 addresses.
    edit <name>
        set uuid {uuid}
        set subnet {ipv4-classnet-any}
        set type [ipmask|iprange|...]
        set route-tag {integer}
        set sub-type [sdn|fsso|...]
        set clearpass-spt [unknown|healthy|...]
        set start-ip {ipv4-address-any}
        set end-ip {ipv4-address-any}
        set fqdn {string}
        set country {string}
        set wildcard-fqdn {string}
        set pattern-start {integer}
        set pattern-end {integer}
        set cache-ttl {integer}
        set wildcard {ipv4-classnet-any}
        set sdn {string}
        set fsso-group <name1>, <name2>, ...
        set interface {string}
        set tenant {string}
        set organization {string}
        set epg-name {string}
        set subnet-name {string}
        set sdn-tag {string}
        set policy-group {string}
        set obj-tag {string}
        set obj-type [ip|mac]
        set tag-detection-level {string}
        set tag-type {string}
        set hw-vendor {string}
        set hw-model {string}
        set os {string}
        set sw-version {string}
        set comment {var-string}
        set associated-interface {string}
        set color {integer}
        set filter {var-string}
        set sdn-addr-type [private|public|...]
        set node-ip-only [enable|disable]
        set obj-id {var-string}
    config list
        Description: IP address list.
        edit <ip>
        next
    end
    config tagging
        Description: Config object tagging.
        edit <name>
            set category {string}
            set tags <name1>, <name2>, ...

```

```

        next
    end
    set allow-routing [enable|disable]
    set fabric-object [enable|disable]
next
end

```

config firewall address

Parameter	Description	Type	Size	Default
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
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
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>fqdn-group</i>	Fully Qualified Domain Name Group 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.		
	<i>interface-subnet</i>	IP and subnet of interface.		
route-tag	route-tag address.	integer	Minimum value: 1 Maximum value: 4294967295	0
sub-type	Sub-type of address.	option	-	sdn

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sdn</i></td><td>SDN address.</td></tr><tr><td><i>fsso</i></td><td>FSSO address.</td></tr><tr><td><i>ems-tag</i></td><td>FortiClient EMS tag.</td></tr><tr><td><i>fortinac-tag</i></td><td>FortiNAC tag.</td></tr></table>	Option	Description	<i>sdn</i>	SDN address.	<i>fsso</i>	FSSO address.	<i>ems-tag</i>	FortiClient EMS tag.	<i>fortinac-tag</i>	FortiNAC tag.							
	Option	Description																
	<i>sdn</i>	SDN address.																
	<i>fsso</i>	FSSO address.																
	<i>ems-tag</i>	FortiClient EMS tag.																
<i>fortinac-tag</i>	FortiNAC tag.																	
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unknown</i></td><td>UNKNOWN.</td></tr><tr><td><i>healthy</i></td><td>HEALTHY.</td></tr><tr><td><i>quarantine</i></td><td>QUARANTINE.</td></tr><tr><td><i>checkup</i></td><td>CHECKUP.</td></tr><tr><td><i>transient</i></td><td>TRANSIENT.</td></tr><tr><td><i>infected</i></td><td>INFECTED.</td></tr></table>	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.			
	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.																	
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255															
country	IP addresses associated to a specific country.	string	Maximum length: 2															
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255															
pattern-start	Starting number of pattern for fqdn-group.	integer	Minimum value: 0 Maximum value: 65535	0														
pattern-end	Ending number of pattern for fqdn-group.	integer	Minimum value: 0 Maximum value: 65535	0														

Parameter	Description	Type	Size	Default
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400	0
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
sdn	SDN.	string	Maximum length: 35	
fsso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511	
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35	
tenant	Tenant.	string	Maximum length: 35	
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35	
epg-name	Endpoint group name.	string	Maximum length: 255	
subnet-name	Subnet name.	string	Maximum length: 255	
sdn-tag	SDN Tag.	string	Maximum length: 15	
policy-group	Policy group name.	string	Maximum length: 15	
obj-tag	Tag of dynamic address object.	string	Maximum length: 255	
obj-type	Object type.	option	-	ip
	Option Description			
	<i>ip</i>	IP address.		
	<i>mac</i>	MAC address		
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	

Parameter	Description	Type	Size	Default								
hw-vendor	Dynamic address matching hardware vendor.	string	Maximum length: 35									
hw-model	Dynamic address matching hardware model.	string	Maximum length: 35									
os	Dynamic address matching operating system.	string	Maximum length: 35									
sw-version	Dynamic address matching software version.	string	Maximum length: 35									
comment	Comment.	var-string	Maximum length: 255									
associated-interface	Network interface associated with address.	string	Maximum length: 35									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0								
filter	Match criteria filter.	var-string	Maximum length: 2047									
sdn-addr-type	Type of addresses to collect.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private</i></td><td>Collect private addresses only.</td></tr><tr><td><i>public</i></td><td>Collect public addresses only.</td></tr><tr><td><i>all</i></td><td>Collect both public and private addresses.</td></tr></table>				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.
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.											
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><i>enable</i></td><td>Enable collection of node addresses only in Kubernetes.</td></tr><tr><td><i>disable</i></td><td>Disable collection of node addresses only in Kubernetes.</td></tr></table>				Option	Description	<i>enable</i>	Enable collection of node addresses only in Kubernetes.	<i>disable</i>	Disable collection of node addresses only in Kubernetes.		
Option	Description											
<i>enable</i>	Enable collection of node addresses only in Kubernetes.											
<i>disable</i>	Disable collection of node addresses only in Kubernetes.											
obj-id	Object ID for NSX.	var-string	Maximum length: 255									
allow-routing	Enable/disable use of this address in the static route configuration.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable use of this address in the static route configuration.		
	<i>disable</i>	Disable use of this address in the static route configuration.		
fabric-object	Security Fabric global object setting.	option	-	disable
	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.		

config list

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

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	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 uuid {uuid}
    set type [ipprefix|iprange|...]
    set route-tag {integer}
    set sdn {string}
    set ip6 {ipv6-network}
    set start-ip {ipv6-address}
```

```

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

```

config firewall address6

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default														
type	Type of IPv6 address object (default = ipprefix).	option	-	ipprefix														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipprefix</td><td>Uses the IP prefix to define a range of IPv6 addresses.</td></tr><tr><td>iprange</td><td>Range of IPv6 addresses between two specified addresses (inclusive).</td></tr><tr><td>fqdn</td><td>Fully qualified domain name.</td></tr><tr><td>geography</td><td>IPv6 addresses from a specified country.</td></tr><tr><td>dynamic</td><td>Dynamic address object for SDN.</td></tr><tr><td>route-tag</td><td>route-tag addresses.</td></tr></table>	Option	Description	ipprefix	Uses the IP prefix to define a range of IPv6 addresses.	iprange	Range of IPv6 addresses between two specified addresses (inclusive).	fqdn	Fully qualified domain name.	geography	IPv6 addresses from a specified country.	dynamic	Dynamic address object for SDN.	route-tag	route-tag addresses.			
	Option	Description																
	ipprefix	Uses the IP prefix to define a range of IPv6 addresses.																
	iprange	Range of IPv6 addresses between two specified addresses (inclusive).																
	fqdn	Fully qualified domain name.																
	geography	IPv6 addresses from a specified country.																
	dynamic	Dynamic address object for SDN.																
route-tag	route-tag addresses.																	
route-tag	route-tag address.	integer	Minimum value: 1 Maximum value: 4294967295	0														
sdn	SDN.	string	Maximum length: 35															
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified	::/0														
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx x).	ipv6-address	Not Specified	::														
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx x).	ipv6-address	Not Specified	::														
fqdn	Fully qualified domain name.	string	Maximum length: 255															
country	IPv6 addresses associated to a specific country.	string	Maximum length: 2															
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400	0														

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								
obj-id	Object ID for NSX.	var-string	Maximum length: 255									
comment	Comment.	var-string	Maximum length: 255									
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.											
host	Host Address.	ipv6-address	Not Specified	::								
tenant	Tenant.	string	Maximum length: 35									
epg-name	Endpoint group name.	string	Maximum length: 255									
sdn-tag	SDN Tag.	string	Maximum length: 15									
filter	Match criteria filter.	var-string	Maximum length: 2047									
sdn-addr-type	Type of addresses to collect.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private</i></td><td>Collect private addresses only.</td></tr><tr><td><i>public</i></td><td>Collect public addresses only.</td></tr><tr><td><i>all</i></td><td>Collect both public and private addresses.</td></tr></table>				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.
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.											
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.											

config list

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

config tagging

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

config subnet-segment

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 63	
type	Subnet segment type.	option	-	any
	Option	Description		
	<i>any</i>	Wildcard.		
	<i>specific</i>	Specific subnet segment address.		
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 type [default|folder]
    set category [default|ztna-ems-tag|...]
    set uuid {uuid}
    set allow-routing [enable|disable]
    set member <name1>, <name2>, ...
```

```

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

```

config firewall addrgrp

Parameter	Description	Type	Size	Default								
name	Address group name.	string	Maximum length: 79									
type	Address group type.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Default address group type (address may belong to multiple groups).</td></tr><tr><td><i>folder</i></td><td>Address folder group (members may not belong to any other group).</td></tr></table>	Option	Description	<i>default</i>	Default address group type (address may belong to multiple groups).	<i>folder</i>	Address folder group (members may not belong to any other group).					
Option	Description											
<i>default</i>	Default address group type (address may belong to multiple groups).											
<i>folder</i>	Address folder group (members may not belong to any other group).											
category	Address group category.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Default address group category (cannot be used as ztna-ems-tag in policy).</td></tr><tr><td><i>ztna-ems-tag</i></td><td>Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.</td></tr><tr><td><i>ztna-geo-tag</i></td><td>Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.</td></tr></table>	Option	Description	<i>default</i>	Default address group category (cannot be used as ztna-ems-tag in policy).	<i>ztna-ems-tag</i>	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.	<i>ztna-geo-tag</i>	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.			
Option	Description											
<i>default</i>	Default address group category (cannot be used as ztna-ems-tag in policy).											
<i>ztna-ems-tag</i>	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.											
<i>ztna-geo-tag</i>	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.											
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000								
allow-routing	Enable/disable use of this group in the static route configuration.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable use of this group in the static route configuration.		
	<i>disable</i>	Disable use of this group in the static route configuration.		
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
exclude	Enable/disable address exclusion.	option	-	disable
	Option Description			
	<i>enable</i>	Enable address exclusion.		
	<i>disable</i>	Disable address exclusion.		
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79	
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			
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	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 uuid {uuid}
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set fabric-object [enable|disable]
  next
end
```

config firewall addrgrp6

Parameter	Description	Type	Size	Default
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
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	
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79	
exclude	Enable/disable address6 exclusion.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable address6 exclusion.		
	<i>disable</i>	Disable address6 exclusion.		
exclude-member <name>	Address6 exclusion member. Address6 name.	string	Maximum length: 79	
fabric-object	Security Fabric global object setting.	option	-	disable
	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.		

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	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 portal-addr {string}
  set portal-addr6 {string}
  set identity-based-route {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	
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	
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35	
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 central SNAT policies.

```
config firewall central-snat-map
  Description: Configure central SNAT policies.
  edit <policyid>
    set status [enable|disable]
    set action [bypass|masquerade|...]
    set ipv6 [enable|disable]
    set srcintf {string}
    set dstintf {string}
    set src-addr <name1>, <name2>, ...
    set src-addr6 <name1>, <name2>, ...
    set dst-addr <name1>, <name2>, ...
    set dst-addr6 <name1>, <name2>, ...
    set nat-ippool <name1>, <name2>, ...
    set nat-ippool6 <name1>, <name2>, ...
  next
end
```


config firewall central-snat-map

Parameter	Description	Type	Size	Default								
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
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.											
action	central SNAT action.	option	-	masquerade								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass and do not perform NAT.</td></tr><tr><td><i>masquerade</i></td><td>NAT using the primary IP of destination interface.</td></tr><tr><td><i>ippool</i></td><td>NAT using ip pool.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass and do not perform NAT.	<i>masquerade</i>	NAT using the primary IP of destination interface.	<i>ippool</i>	NAT using ip pool.			
	Option	Description										
	<i>bypass</i>	Bypass and do not perform NAT.										
	<i>masquerade</i>	NAT using the primary IP of destination interface.										
<i>ippool</i>	NAT using ip pool.											
ipv6	Enable/disable IPv6.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ipv6.</td></tr><tr><td><i>disable</i></td><td>Disable ipv6.</td></tr></table>	Option	Description	<i>enable</i>	Enable ipv6.	<i>disable</i>	Disable ipv6.					
	Option	Description										
	<i>enable</i>	Enable ipv6.										
<i>disable</i>	Disable ipv6.											
srcintf	Source interface name from available interfaces.	string	Maximum length: 35									
dstintf	Destination interface name from available interfaces.	string	Maximum length: 35									
src-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79									
src-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79									
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79									
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79									

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	

config firewall city

Define city table.

```
config firewall city
    Description: Define city table.
    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.

```
config firewall country
    Description: Define country table.
    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 traffic-type {option1}, {option2}, ...
    set traffic-source [client|server|...]
    set interface <name1>, <name2>, ...
  next
end
```

config firewall decrypted-traffic-mirror

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
dstmac	Set destination MAC address for mirrored traffic.	mac-address	Not Specified	ff:ff:ff:ff:ff:ff
traffic-type	Types of decrypted traffic to be mirrored.	option	-	ssl

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	Mirror decrypted SSL traffic.		
	<i>ssh</i>	Mirror decrypted SSH traffic.		
traffic-source	Source of decrypted traffic to be mirrored.	option	-	client
	Option	Description		
	<i>client</i>	Mirror client side decrypted traffic.		
	<i>server</i>	Mirror server side decrypted traffic.		
	<i>both</i>	Mirror both client and server side decrypted traffic.		
interface <name>	Decrypted traffic mirror interface. Decrypted traffic mirror interface.	string	Maximum length: 79	

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	Persistence 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 gateway {ipv4-address}
        set device {string}
        set groups <name1>, <name2>, ...
      next
    end
  next
end
```

config firewall identity-based-route

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

config rule

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
gateway	IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx , Default: 0.0.0.0).	ipv4-address	Not Specified	0.0.0.0
device	Outgoing interface for the rule.	string	Maximum length: 35	
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	

config firewall internet-service

Show Internet Service application.

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

config firewall internet-service

Parameter	Description	Type	Size	Default								
id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
name	Internet Service name.	string	Maximum length: 63									
icon-id	Icon ID of Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	0								
direction	How this service may be used in a firewall policy (source, destination or both).	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>src</td><td>As source in the firewall policy.</td></tr><tr><td>dst</td><td>As destination in the firewall policy.</td></tr><tr><td>both</td><td>Both directions in the firewall policy.</td></tr></table>				Option	Description	src	As source in the firewall policy.	dst	As destination in the firewall policy.	both	Both directions in the firewall policy.
Option	Description											
src	As source in the firewall policy.											
dst	As destination in the firewall policy.											
both	Both directions in the firewall policy.											

Parameter	Description	Type	Size	Default						
database	Database name this Internet Service belongs to.	option	-	isdb						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>isdb</td><td>Internet Service Database.</td></tr><tr><td>irdb</td><td>Internet RRR Database.</td></tr></table>				Option	Description	isdb	Internet Service Database.	irdb	Internet RRR Database.
	Option	Description								
	isdb	Internet Service Database.								
irdb	Internet RRR Database.									
ip-range-number	Number of IPv4 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0						
extra-ip-range-number	Extra number of IPv4 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-number	Total number of IPv4 addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip6-range-number	Number of IPv6 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0						
extra-ip6-range-number	Extra number of IPv6 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0						
singularity	Singular level of the Internet Service.	integer	Minimum value: 0 Maximum value: 65535	0						
obsolete	Indicates whether the Internet Service can be used.	integer	Minimum value: 0 Maximum value: 255	0						

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]
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      next
    end
  next
end
```

config firewall internet-service-addition

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

config entry

Parameter	Description	Type	Size	Default
id	Entry ID(1-255).	integer	Minimum value: 0 Maximum value: 255	0
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.		
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6

config port-range

Parameter	Description	Type	Size	Default
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
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

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 match-port {integer}
  set append-port {integer}
end
```

config firewall internet-service-append

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

config firewall internet-service-botnet

Show Internet Service botnet.

```
config firewall internet-service-botnet
  Description: Show Internet Service botnet.
  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 reputation {integer}
    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 protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
        set dst <name1>, <name2>, ...
        set dst6 <name1>, <name2>, ...
      next
    end
  next
end
```

config firewall internet-service-custom

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

config entry

Parameter	Description	Type	Size	Default
id	Entry ID(1-255).	integer	Minimum value: 0 Maximum value: 255	0
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	ipv4	IPv4 mode.		
	ipv6	IPv6 mode.		
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6
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	

config port-range

Parameter	Description	Type	Size	Default
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
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

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

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}
        set protocol {integer}
        config port-range
          Description: Port ranges in the definition entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      next
    end
  next
end
```

```
next
end
```

config firewall internet-service-definition

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

config entry

Parameter	Description	Type	Size	Default
seq-num	Entry sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
category-id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	
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
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

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

```

```

        edit <id>
            set start-ip {ipv4-address-any}
            set end-ip {ipv4-address-any}
        next
    end
    config ip6-range
        Description: IPv6 ranges in the disable entry.
        edit <id>
            set start-ip6 {ipv6-address}
            set end-ip6 {ipv6-address}
        next
    end
next
end
next
end

```

config firewall internet-service-extension

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

config entry

Parameter	Description	Type	Size	Default						
id	Entry ID(1-255).	integer	Minimum value: 0 Maximum value: 255	0						
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
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6
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	

config port-range

Parameter	Description	Type	Size	Default
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
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config disable-entry

Parameter	Description	Type	Size	Default				
id	Disable entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0				
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></table>				Option	Description	ipv4	IPv4 mode.
Option	Description							
ipv4	IPv4 mode.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ipv6</i>	IPv6 mode.		
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
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
end-port	Ending TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config ip-range

Parameter	Description	Type	Size	Default
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
end-ip	End IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0

config ip6-range

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	::
end-ip6	End IPv6 address.	ipv6-address	Not Specified	::

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
name	Internet Service group name.	string	Maximum length: 63	
comment	Comment.	var-string	Maximum length: 255	
direction	How this service may be used (source, destination or both).	option	-	both
		Option	Description	
		source	As source when applied.	
		destination	As destination when applied.	
		both	Both directions when applied.	

Parameter	Description	Type	Size	Default
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79	

config firewall internet-service-ipbl-reason

IP block list reason.

```
config firewall internet-service-ipbl-reason
  Description: IP block list reason.
  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	0
name	IP block list reason name.	string	Maximum length: 63	

config firewall internet-service-ipbl-vendor

IP block list vendor.

```
config firewall internet-service-ipbl-vendor
  Description: IP block list vendor.
  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.

```
config firewall internet-service-list
  Description: Internet Service list.
  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 type [default|location]
```

```

        set internet-service-id {integer}
        set country-id {integer}
        set region-id {integer}
        set city-id {integer}
    next
end

```

config firewall internet-service-name

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

config firewall internet-service-owner

Internet Service owner.

```
config firewall internet-service-owner
  Description: Internet Service owner.
  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.

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

config firewall internet-service-reputation

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

config firewall internet-service-sld

Internet Service Second Level Domain.

```
config firewall internet-service-sld
  Description: Internet Service Second Level Domain.
  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 Maximum value: 4294967295	0
name	Second Level Domain name.	string	Maximum length: 63	

config firewall internet-service-subapp

Show Internet Service sub app ID.

```
config firewall internet-service-subapp
  Description: Show Internet Service sub app ID.
  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 Maximum value: 4294967295	0

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

config firewall ippool

Configure IPv4 IP pools.

```
config firewall ippool
  Description: Configure IPv4 IP pools.
  edit <name>
    set startip {ipv4-address-any}
    set endip {ipv4-address-any}
    set comments {var-string}
  next
end
```

config firewall ippool

Parameter	Description	Type	Size	Default
name	IP pool name.	string	Maximum length: 79	
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
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
comments	Comment.	var-string	Maximum length: 255	

config firewall ippool6

Configure IPv6 IP pools.

```
config firewall ippool6
  Description: Configure IPv6 IP pools.
  edit <name>
    set startip {ipv6-address}
```

```

    set endip {ipv6-address}
    set comments {var-string}
    set nat46 [disable|enable]
    set add-nat46-route [disable|enable]
next
end

```

config firewall ippool6

Parameter	Description	Type	Size	Default						
name	IPv6 IP pool name.	string	Maximum length: 79							
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	::						
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	::						
comments	Comment.	var-string	Maximum length: 255							
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.									
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable adding NAT46 route.</td></tr><tr><td>enable</td><td>Enable adding NAT46 route.</td></tr></table>				Option	Description	disable	Disable adding NAT46 route.	enable	Enable adding NAT46 route.
Option	Description									
disable	Disable adding NAT46 route.									
enable	Enable adding NAT46 route.									

config firewall network-service-dynamic

Configure Dynamic Network Services.

```

config firewall network-service-dynamic
    Description: Configure Dynamic Network Services.

```

```

edit <name>
    set sdn {string}
    set comment {var-string}
    set filter {var-string}
next
end

```

config firewall network-service-dynamic

Parameter	Description	Type	Size	Default
name	Dynamic Network Service name.	string	Maximum length: 63	
sdn	SDN connector name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
filter	Match criteria filter.	var-string	Maximum length: 2047	

config firewall on-demand-sniffer

Configure on-demand packet sniffer.

```

config firewall on-demand-sniffer
    Description: Configure on-demand packet sniffer.
    edit <name>
        set interface <name1>, <name2>, ...
        set max-packet-count {integer}
        set hosts <host1>, <host2>, ...
        set hostnames <hostname1>, <hostname2>, ...
        set snapshot-length {integer}
        set ports <port1>, <port2>, ...
        set protocols <protocol1>, <protocol2>, ...
        set non-ip-packet [enable|disable]
        set advanced-filter {var-string}
    next
end

```

config firewall on-demand-sniffer

Parameter	Description	Type	Size	Default						
name	On-demand packet sniffer name.	string	Maximum length: 35							
interface <name>	Interface names that on-demand packet sniffer will take place. Interface name.	string	Maximum length: 79							
max-packet-count	Maximum number of packets to capture per on-demand packet sniffer.	integer	Minimum value: 1 Maximum value: 20000	0						
hosts <host>	IPv4 or IPv6 hosts to filter in this traffic sniffer. IPv4 or IPv6 host.	string	Maximum length: 255							
hostnames <hostname>	Hostnames to filter in this traffic sniffer. Hostname.	string	Maximum length: 255							
snapshot-length	Maximum number of bytes to capture per packet.	integer	Minimum value: 1 Maximum value: 262144	1600						
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							
non-ip-packet	Include non-IP packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable non-IP packets to be included capture.</td></tr><tr><td><i>disable</i></td><td>Disable non-IP packets to be included in capture.</td></tr></table>				Option	Description	<i>enable</i>	Enable non-IP packets to be included capture.	<i>disable</i>	Disable non-IP packets to be included in capture.
Option	Description									
<i>enable</i>	Enable non-IP packets to be included capture.									
<i>disable</i>	Disable non-IP packets to be included in capture.									
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							

config firewall policy

Configure firewall policies.

```
config firewall policy
  Description: Configure firewall policies.
  edit <policyid>
    set type [explicit-web|transparent|...]
    set status [enable|disable]
    set name {string}
    set uuid {uuid}
    set force-proxy [enable|disable]
    set implicit-proxy-detection [enable|disable]
    set dynamic-bypass [enable|disable]
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set ztna-device-ownership [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set action [accept|deny|...]
    set schedule {string}
    set policy-expiry [enable|disable]
    set policy-expiry-date {datetime}
    set service <name1>, <name2>, ...
    set explicit-web-proxy <name1>, <name2>, ...
    set transparent [enable|disable]
    set access-proxy <name1>, <name2>, ...
    set ztna-proxy <name1>, <name2>, ...
    set ztna-ems-tag <name1>, <name2>, ...
    set ztna-ems-tag-secondary <name1>, <name2>, ...
    set ztna-tags-match-logic [or|and]
    set device-ownership [enable|disable]
    set pass-through [enable|disable]
    set url-category <id1>, <id2>, ...
    set url-risk <name1>, <name2>, ...
    set internet-service [enable|disable]
    set internet-service-name <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-custom <name1>, <name2>, ...
    set internet-service6 [enable|disable]
    set internet-service6-name <name1>, <name2>, ...
    set internet-service6-group <name1>, <name2>, ...
    set internet-service6-custom <name1>, <name2>, ...
    set internet-service6-custom-group <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set utm-status [enable|disable]
    set ztna-policy-redirect [enable|disable]
    set webproxy-profile {string}
    set logtraffic [all|utm|...]
```

```
set logtraffic-start [enable|disable]
set log-http-transaction [disable|enable]
set extended-log [enable|disable]
set wanopt [enable|disable]
set wanopt-detection [active|passive|...]
set wanopt-passive-opt [default|transparent|...]
set wanopt-profile {string}
set wanopt-peer {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set reverse-cache [disable|enable]
set http-tunnel-auth [enable|disable]
set ssh-policy-check [enable|disable]
set webproxy-forward-server {string}
set isolator-server {string}
set poolname <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set disclaimer [disable|domain|...]
set comments {var-string}
set redirect-url {var-string}
set custom-log-fields <field-id1>, <field-id2>, ...
set replacemsg-override-group {string}
set srcaddr-negate [enable|disable]
set dstaddr-negate [enable|disable]
set service-negate [enable|disable]
set internet-service-negate [enable|disable]
set internet-service6-negate [enable|disable]
set application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
set https-sub-category [enable|disable]
set decrypted-traffic-mirror {string}
set max-session-per-user {integer}
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set ia-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-profile {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set icap-profile {string}
set cifs-profile {string}
set videofilter-profile {string}
set isolator-profile {string}
set redirect-profile {string}
```

```

set ssh-filter-profile {string}
set casb-profile {string}
set detect-https-in-http-request [enable|disable]
set service-connector {string}
next
end

```

config firewall policy

Parameter	Description	Type	Size	Default
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0
type	Type of policy.	option	-	transparent
	Option Description			
	<i>explicit-web</i>	Explicit Web Proxy policy		
	<i>transparent</i>	Transparent firewall policy		
	<i>explicit-ftp</i>	Explicit FTP Proxy policy		
	<i>ssh-tunnel</i>	SSH Tunnel policy		
	<i>ssh</i>	SSH policy		
	<i>access-proxy</i>	Access Proxy		
	<i>ztna-proxy</i>	ZTNA Proxy		
	<i>wanopt</i>	WANopt Tunnel		
status	Enable or disable this policy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	Policy name.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
force-proxy	Force proxy.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Force all TCP transparent traffic to proxy.		
	<i>disable</i>	Do not force TCP transparent traffic to proxy.		
implicit-proxy-detection	Implicit proxy detection.	option	-	disable
	Option Description			
	<i>enable</i>	Enable implicit proxy detection.		
	<i>disable</i>	Disable implicit proxy detection.		
dynamic-bypass	Dynamic bypass.	option	-	disable
	Option Description			
	<i>enable</i>	Enable dynamic bypass to all HTTP traffic in this policy.		
	<i>disable</i>	Disable dynamic bypass to all HTTP traffic in this policy.		
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
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.		
srcaddr <name>	Source address and address group names. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79	
srcaddr6 <name>	IPv6 source address (web proxy and ftp proxy only). Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default										
dstaddr6 <name>	IPv6 destination address (web proxy and ftp proxy only). Address name.	string	Maximum length: 79											
action	Policy action (allow/deny).	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>redirect</i></td><td>Redirect sessions that match the firewall policy to a url.</td></tr><tr><td><i>isolate</i></td><td>Isolate sessions that match the firewall policy with isolator.</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>redirect</i>	Redirect sessions that match the firewall policy to a url.	<i>isolate</i>	Isolate sessions that match the firewall policy with isolator.			
Option	Description													
<i>accept</i>	Allows session that match the firewall policy.													
<i>deny</i>	Blocks sessions that match the firewall policy.													
<i>redirect</i>	Redirect sessions that match the firewall policy to a url.													
<i>isolate</i>	Isolate sessions that match the firewall policy with isolator.													
schedule	Schedule name.	string	Maximum length: 35											
policy-expiry	Enable/disable policy expiry.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy expiry.</td></tr><tr><td><i>disable</i></td><td>Disable polcy expiry.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy expiry.	<i>disable</i>	Disable polcy expiry.							
Option	Description													
<i>enable</i>	Enable policy expiry.													
<i>disable</i>	Disable polcy expiry.													
policy-expiry-date	Policy expiry date (YYYY-MM-DD HH:MM:SS).	datetime	Not Specified	0000-00-00 00:00:00										
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79											
explicit-web-proxy <name>	Explicit web proxy. Explicit Web proxy name.	string	Maximum length: 79											
transparent	set webproxy to use original client address.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using original client address for webproxy.</td></tr><tr><td><i>disable</i></td><td>Disable using original client address for webproxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable using original client address for webproxy.	<i>disable</i>	Disable using original client address for webproxy.							
Option	Description													
<i>enable</i>	Enable using original client address for webproxy.													
<i>disable</i>	Disable using original client address for webproxy.													
access-proxy <name>	Access Proxy. Access Proxy name.	string	Maximum length: 79											
ztna-proxy <name>	ZTNA Traffic Forward Proxy. ZTNA Traffic Forward Proxy name.	string	Maximum length: 79											

Parameter	Description	Type	Size	Default						
ztna-ems-tag <name>	Source ztna-ems-tag names. Address name.	string	Maximum length: 79							
ztna-ems-tag-secondary <name>	Source ztna-ems-tag-secondary names. Address 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><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.									
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.									
pass-through	Enable/disable policy matching pass through	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy matching pass through.</td></tr><tr><td><i>disable</i></td><td>Disable policy matching pass through.</td></tr></table>				Option	Description	<i>enable</i>	Enable policy matching pass through.	<i>disable</i>	Disable policy matching pass through.
Option	Description									
<i>enable</i>	Enable policy matching pass through.									
<i>disable</i>	Disable policy matching pass through.									
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295							
url-risk <name>	URL risk level name. Risk level name.	string	Maximum length: 79							
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	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 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-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-custom <name>	Custom Internet Service Name. Custom Internet Service name.	string	Maximum length: 79							
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><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-name <name>	IPv6 Internet Service name. IPv6 Internet Service name.	string	Maximum length: 79							
internet-service6-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
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-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default								
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	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.											
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>enable</td><td>Enable ZTNA proxy-policy redirect.</td></tr><tr><td>disable</td><td>Disable ZTNA proxy-policy redirect.</td></tr></table>	Option	Description	enable	Enable ZTNA proxy-policy redirect.	disable	Disable ZTNA proxy-policy redirect.					
Option	Description											
enable	Enable ZTNA proxy-policy redirect.											
disable	Disable ZTNA proxy-policy redirect.											
webproxy-profile	Web proxy profile using when none matched policy.	string	Maximum length: 63									
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>Log all sessions accepted or denied 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	Log all sessions accepted or denied by this policy.	utm	Log traffic that has a security profile applied to it.	disable	Disable all logging for this policy.			
Option	Description											
all	Log all sessions accepted or denied by this policy.											
utm	Log traffic that has a security profile applied to it.											
disable	Disable all logging for this policy.											
logtraffic-start	Record logs when a session starts and ends.	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.											
log-http-transaction	Enable/disable http transaction log.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable HTTP transaction log.</td></tr><tr><td>enable</td><td>Enable HTTP transaction log.</td></tr></table>	Option	Description	disable	Disable HTTP transaction log.	enable	Enable HTTP transaction log.					
Option	Description											
disable	Disable HTTP transaction log.											
enable	Enable HTTP transaction log.											

Parameter	Description	Type	Size	Default								
extended-log	Enable/disable extended log for http transaction.	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	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 FortiProxy 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 FortiProxy 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 FortiProxy address to connect to server.											
wanopt-profile	WAN optimization profile.	string	Maximum length: 35									
wanopt-peer	WAN optimization peer.	string	Maximum length: 35									
webcache	Enable/disable web cache.	option	-	disable								

Parameter	Description	Type	Size	Default
	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.		
reverse-cache	Enable/disable reverse cache servers.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable reverse cache.		
	<i>enable</i>	Enable reverse cache servers.		
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ssh-policy-check	Enable/disable SSH policy check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSH policy check.		
	<i>disable</i>	Disable SSH policy check.		
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63	
isolator-server	isolator server name.	string	Maximum length: 63	
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default										
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79											
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											
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													
comments	Comment.	var-string	Maximum length: 1023											
redirect-url	Redirect URL for further web proxy processing.	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											
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35											
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><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable source address negate.</td></tr></table>				Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.				
Option	Description													
<i>enable</i>	Enable source address negate.													
<i>disable</i>	Disable source address negate.													
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable negated service match.		
	<i>disable</i>	Disable negated service match.		
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable negated Internet Service match.		
	<i>disable</i>	Disable negated Internet Service match.		
internet-service6-negate	When enabled internet-service6 specifies what the service must not be.	option	-	disable
	Option Description			
	<i>enable</i>	Enable negated IPv6 Internet Service match.		
	<i>disable</i>	Disable negated IPv6 Internet Service match.		
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-category <id>	Application category ID list. 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	

Parameter	Description	Type	Size	Default						
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.									
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
max-session-per-user	Max UTM sessions per user.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
profile-group	Name of profile group.	string	Maximum length: 35							
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default						
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35							
ia-profile	Image analyzer profile.	string	Maximum length: 35							
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35							
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 35							
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35							
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35							
application-list	Name of an existing Application list.	string	Maximum length: 35							
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35							
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35							
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35							
isolator-profile	Name of an existing isolator profile.	string	Maximum length: 35							
redirect-profile	Name of an existing URL Redirect profile.	string	Maximum length: 35							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35							
casb-profile	Name of an existing CASB profile.	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.									
service-connector	Service Connector.	string	Maximum length: 79							

config firewall profile-group

Configure profile groups.

```
config firewall profile-group
    Description: Configure profile groups.
```

```

edit <name>
    set profile-protocol-options {string}
    set ssl-ssh-profile {string}
    set av-profile {string}
    set ia-profile {string}
    set webfilter-profile {string}
    set dnsfilter-profile {string}
    set emailfilter-profile {string}
    set dlp-profile {string}
    set file-filter-profile {string}
    set ips-sensor {string}
    set application-list {string}
    set icap-profile {string}
    set cifs-profile {string}
    set videofilter-profile {string}
    set isolator-profile {string}
    set redirect-profile {string}
    set ssh-filter-profile {string}
    set casb-profile {string}
next
end

```

config firewall profile-group

Parameter	Description	Type	Size	Default
name	Profile group name.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	certificate-inspection
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
ia-profile	Image analyzer profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
application-list	Name of an existing Application list.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
isolator-profile	Name of an existing isolator profile.	string	Maximum length: 35	
redirect-profile	Name of an existing URL Redirect profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
casb-profile	Name of an existing CASB profile.	string	Maximum length: 35	

config firewall profile-protocol-options

Configure protocol options.

```

config firewall profile-protocol-options
  Description: Configure protocol options.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set oversize-log [disable|enable]
    set switching-protocols-log [disable|enable]
    config proxy-redirect
      Description: Configure proxy redirection protocol options.
      set ports {integer}
      set status [enable|disable]
    end
  config http
    Description: Configure HTTP protocol options.

```

```

set ports {integer}
set status [enable|disable]
set options {option1}, {option2}, ...
set comfort-interval {integer}
set comfort-amount {integer}
set range-block [disable|enable]
set strip-x-forwarded-for [disable|enable]
set post-lang {option1}, {option2}, ...
set streaming-content-bypass [enable|disable]
set dns-protection [enable|disable]
set switching-protocols [bypass|block]
set unknown-http-version [reject|tunnel|...]
set tunnel-non-http [enable|disable]
set h2c [enable|disable]
set unknown-content-encoding [block|inspect|...]
set oversize-limit {integer}
set uncompressed-oversize-limit {integer}
set uncompressed-nest-limit {integer}
set stream-based-uncompressed-limit {integer}
set scan-bzip2 [enable|disable]
set verify-dns-for-policy-matching [enable|disable]
set block-page-status-code {integer}
set retry-count {integer}
set domain-fronting [allow|block|...]
set tcp-window-type [auto-tuning|system|...]
set tcp-window-minimum {integer}
set tcp-window-maximum {integer}
set tcp-window-size {integer}
set ssl-offloaded [no|yes]
set address-ip-rating [enable|disable]
set encrypted-file [pass|inspect|...]
set encrypted-file-log [enable|disable]
end
config ftp
  Description: Configure FTP protocol options.
  set ports {integer}
  set status [enable|disable]
  set options {option1}, {option2}, ...
  set comfort-interval {integer}
  set comfort-amount {integer}
  set oversize-limit {integer}
  set uncompressed-oversize-limit {integer}
  set uncompressed-nest-limit {integer}
  set stream-based-uncompressed-limit {integer}
  set scan-bzip2 [enable|disable]
  set tcp-window-type [auto-tuning|system|...]
  set tcp-window-minimum {integer}
  set tcp-window-maximum {integer}
  set tcp-window-size {integer}
  set ssl-offloaded [no|yes]
  set explicit-ftp-tls [enable|disable]
end

```

```

config imap
    Description: Configure IMAP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set address-ip-rating [enable|disable]
end
config mapi
    Description: Configure MAPI protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
config pop3
    Description: Configure POP3 protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
end
config smtp
    Description: Configure SMTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set server-busy [enable|disable]
    set ssl-offloaded [no|yes]
end
config nntp
    Description: Configure NNTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}

```

```

        set uncompressed-nest-limit {integer}
        set scan-bzip2 [enable|disable]
    end
    config ssh
        Description: Configure SFTP and SCP protocol options.
        set options {option1}, {option2}, ...
        set comfort-interval {integer}
        set comfort-amount {integer}
        set oversize-limit {integer}
        set uncompressed-oversize-limit {integer}
        set uncompressed-nest-limit {integer}
        set stream-based-uncompressed-limit {integer}
        set scan-bzip2 [enable|disable]
        set tcp-window-type [auto-tuning|system|...]
        set tcp-window-minimum {integer}
        set tcp-window-maximum {integer}
        set tcp-window-size {integer}
        set ssl-offloaded [no|yes]
    end
    config dns
        Description: Configure DNS protocol options.
        set ports {integer}
        set status [enable|disable]
    end
    config cifs
        Description: Configure CIFS protocol options.
        set ports {integer}
        set status [enable|disable]
        set options {option1}, {option2}, ...
        set oversize-limit {integer}
        set uncompressed-oversize-limit {integer}
        set uncompressed-nest-limit {integer}
        set scan-bzip2 [enable|disable]
        set tcp-window-type [auto-tuning|system|...]
        set tcp-window-minimum {integer}
        set tcp-window-maximum {integer}
        set tcp-window-size {integer}
        set server-credential-type [none|credential-replication|...]
        set domain-controller {string}
        config server-keytab
            Description: Server keytab.
            edit <principal>
                set keytab {string}
            next
        end
    end
    config mail-signature
        Description: Configure Mail signature.
        set status [disable|enable]
        set signature {string}
    end
    set rpc-over-http [enable|disable]

```

```
next
end
```

config firewall profile-protocol-options

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 35							
comment	Optional comments.	var-string	Maximum length: 255							
replacemsg-group	Name of the replacement message group to be used.	string	Maximum length: 35							
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging for antivirus oversize file blocking.</td></tr><tr><td><i>enable</i></td><td>Enable logging for antivirus oversize file blocking.</td></tr></table>				Option	Description	<i>disable</i>	Disable logging for antivirus oversize file blocking.	<i>enable</i>	Enable logging for antivirus oversize file blocking.
Option	Description									
<i>disable</i>	Disable logging for antivirus oversize file blocking.									
<i>enable</i>	Enable logging for antivirus oversize file blocking.									
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging for HTTP/HTTPS switching protocols.</td></tr><tr><td><i>enable</i></td><td>Enable logging for HTTP/HTTPS switching protocols.</td></tr></table>				Option	Description	<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.	<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.
Option	Description									
<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.									
<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.									
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of RPC over HTTP.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of RPC over HTTP.</td></tr></table>				Option	Description	<i>enable</i>	Enable inspection of RPC over HTTP.	<i>disable</i>	Disable inspection of RPC over HTTP.
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTP.									
<i>disable</i>	Disable inspection of RPC over HTTP.									

config proxy-redirect

Parameter	Description	Type	Size	Default
ports	Ports to inspect all for content (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config http

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	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>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.		
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1
range-block	Enable/disable blocking of partial downloads.	option	-	disable

Parameter	Description	Type	Size	Default
	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)		
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable
	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.		
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	-	
	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.		
	<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.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></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>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>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).															
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															
dns-protection	Enable/disable DNS protection for HTTP/HTTPS traffic.	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.															
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass connections when switching protocols.</td></tr><tr><td><i>block</i></td><td>Block connections when switching protocols.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass connections when switching protocols.	<i>block</i>	Block connections when switching protocols.									
	Option	Description														
	<i>bypass</i>	Bypass connections when switching protocols.														
<i>block</i>	Block connections when switching protocols.															
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></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.									
	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.															

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></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>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>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.											
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><i>enable</i></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><i>disable</i></td><td>Drop or tear down non-HTTP sessions accepted by the profile.</td></tr></table>	Option	Description	<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.					
	Option	Description										
	<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.										
<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.											
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.											
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.											
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10								

Parameter	Description	Type	Size	Default						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10						
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						
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 Maximum value: 4294967295	0						
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.									
verify-dns-for-policy-matching	Enable/disable verify 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.									
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						
retry-count	Number of attempts to retry HTTP connection (0 - 100, default = 0).	integer	Minimum value: 0 Maximum value: 100	0						
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></table>	Option	Description	<i>allow</i>	Allow domain fronting.					
Option	Description									
<i>allow</i>	Allow domain fronting.									

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></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>block</i>	Block and log domain fronting.	<i>monitor</i>	Allow and log domain fronting.							
	Option	Description												
	<i>block</i>	Block and log domain fronting.												
<i>monitor</i>	Allow and log domain fronting.													
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.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144										
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 FortiProxy 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 FortiProxy 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 FortiProxy when deep-inspection is enabled.												
<i>yes</i>	SSL decryption and encryption performed by an external device.													
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
encrypted-file	Encrypted file action (default = pass).	option	-	pass
	Option	Description		
	<i>pass</i>	Pass encrypted files without content scan.		
	<i>inspect</i>	Request password to decrypt and scan encrypted file. Files failed to decrypt will be blocked.		
	<i>block</i>	Block encrypted files.		
encrypted-file-log	Enable/disable Log encrypted file.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config ftp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 21).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	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>clientcomfort</i>	Prevent client timeout.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10
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
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 Maximum value: 4294967295	0
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
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.		
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option	Description		
	<i>no</i>	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		
explicit-ftp-tls	Enable/disable deep inspection of FTP control session over STARTTLS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config imap

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 143).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	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: 4095	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10
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
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						
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 FortiProxy 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 FortiProxy when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.			
Option	Description									
no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.									
yes	SSL decryption and encryption performed by an external device.									
address-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 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 mapi

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content (1 - 65535, default = 135).	integer	Minimum value: 1 Maximum value: 65535							
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.									
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.									

Parameter	Description	Type	Size	Default						
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10						
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						
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.									

config pop3

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content (1 - 65535, default = 110).	integer	Minimum value: 1 Maximum value: 65535							
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.									
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></table>				Option	Description	<i>fragmail</i>	Pass fragmented email.		
	Option	Description								
<i>fragmail</i>	Pass fragmented email.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>oversize</i></td><td>Block oversized email.</td></tr></table>	Option	Description	<i>oversize</i>	Block oversized email.					
	Option	Description								
	<i>oversize</i>	Block oversized email.								
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10						
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						
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 FortiProxy 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 FortiProxy 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 FortiProxy when deep-inspection is enabled.								
<i>yes</i>	SSL decryption and encryption performed by an external device.									

config smtp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 25).	integer	Minimum value: 1 Maximum value: 65535	

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	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: 4095	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10
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
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>no</i>	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

config nntp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 119).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	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>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: 4095	10

Parameter	Description	Type	Size	Default						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10						
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						
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.									

config ssh

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>oversize</i></td><td>Block oversized file.</td></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></table>	Option	Description	<i>oversize</i>	Block oversized file.	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.			
Option	Description											
<i>oversize</i>	Block oversized file.											
<i>clientcomfort</i>	Prevent client timeout.											
<i>servercomfort</i>	Prevent server timeout.											
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10								
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1								
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10								

Parameter	Description	Type	Size	Default										
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10										
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										
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 Maximum value: 4294967295	0										
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.													
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.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										

Parameter	Description	Type	Size	Default
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option	Description		
	no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.		
	yes	SSL decryption and encryption performed by an external device.		

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						
	<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 cifs

Parameter	Description	Type	Size	Default
ports	Ports to scan for content (1 - 65535, default = 445).	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	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>oversize</i>	Block oversized file.		
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 4095	10
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
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning

Parameter	Description	Type	Size	Default
	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.		
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 16777216	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 16777216	262144
server-credential-type	CIFS server credential type.	option	-	none
	Option	Description		
	<i>none</i>	Credential derivation not set.		
	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.		
	<i>credential-keytab</i>	Credential derived using server keytab.		
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63	

config server-keytab

Parameter	Description	Type	Size	Default
principal	Service principal. For example, host/cifsserver.example.com@example.com.	string	Maximum length: 511	
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	

config mail-signature

Parameter	Description	Type	Size	Default
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiProxy.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable mail signature.	
		<i>enable</i>	Enable mail signature.	
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023	

config firewall proxy-address

Configure web proxy address.

```
config firewall proxy-address
  Description: Configure web proxy address.
  edit <name>
    set uuid {uuid}
    set type [host-regex|url|...]
    set host {string}
    set host-regex {string}
    set path {string}
    set query {string}
    set referrer [enable|disable]
    set post-arg [enable|disable]
    set category <id1>, <id2>, ...
    set url-list {string}
    set method {option1}, {option2}, ...
    set ua {option1}, {option2}, ...
    set ua-min-ver {string}
    set ua-max-ver {string}
```

```

set header-name {string}
set header {string}
set case-sensitivity [disable|enable]
config header-group
    Description: HTTP header group.
    edit <id>
        set header-name {string}
        set header {string}
        set case-sensitivity [disable|enable]
    next
end
set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set comment {var-string}
set application <name1>, <name2>, ...
next
end

```

config firewall proxy-address

Parameter	Description	Type	Size	Default
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
type	Proxy address type.	option	-	url

Option	Description
<i>host-regex</i>	Host regular expression.
<i>url</i>	HTTP URL.
<i>category</i>	FortiGuard URL category.
<i>url-list</i>	HTTP URL list from external resource or Web filter URL list.
<i>method</i>	HTTP request method.
<i>ua</i>	HTTP request user agent.
<i>header</i>	HTTP request header.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>src-advanced</i>	HTTP advanced source criteria.		
	<i>dst-advanced</i>	HTTP advanced destination criteria.		
	<i>saas</i>	SaaS application.		
	<i>response-header</i>	HTTP response header.		
host	Address object for the host.	string	Maximum length: 79	
host-regex	Host name as a regular expression.	string	Maximum length: 255	
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
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
post-arg	Enable/disable use of body in the HTTP POST to match the query.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
category <id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
url-list	External or Web filter URL list.	string	Maximum length: 35	
method	HTTP request methods to be used.	option	-	

Parameter	Description	Type	Size	Default																		
	<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></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.			
	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.																					
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-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																			
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																			
header-name	Name of HTTP header.	string	Maximum length: 79																			

Parameter	Description	Type	Size	Default						
header	HTTP header name as a regular expression.	string	Maximum length: 255							
case-sensitivity	Enable to make the pattern case sensitive.	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.									
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							
application <name>	SaaS application. SaaS application name.	string	Maximum length: 79							

config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	disable	Case insensitive in pattern.		
	enable	Case sensitive in pattern.		

config tagging

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

config firewall proxy-address6

Configure web proxy address6.

```
config firewall proxy-address6
  Description: Configure web proxy address6.
  edit <name>
    set uuid {uuid}
    set type [host-regex|url|...]
    set host {string}
    set host-regex {string}
    set path {string}
    set query {string}
    set referrer [enable|disable]
    set post-arg [enable|disable]
    set category <id1>, <id2>, ...
    set url-list {string}
    set method {option1}, {option2}, ...
    set ua {option1}, {option2}, ...
    set ua-min-ver {string}
    set ua-max-ver {string}
    set header-name {string}
    set header {string}
    set case-sensitivity [disable|enable]
  config header-group
    Description: HTTP header group.
    edit <id>
      set header-name {string}
      set header {string}
      set case-sensitivity [disable|enable]
    next
  end
  set color {integer}
  config tagging
    Description: Config object tagging.
    edit <name>
      set category {string}
```

```

        set tags <name1>, <name2>, ...
    next
end
set comment {var-string}
set application <name1>, <name2>, ...
next
end

```

config firewall proxy-address6

Parameter	Description	Type	Size	Default
name	Address6 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
type	Proxy address6 type.	option	-	url
	Option		Description	
	<i>host-regex</i>	Host regular expression.		
	<i>url</i>	HTTP URL.		
	<i>category</i>	FortiGuard URL category.		
	<i>url-list</i>	HTTP URL list from external resource or Web filter URL list.		
	<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.		
	<i>response-header</i>	HTTP response header.		
host	Address6 object for the host.	string	Maximum length: 79	
host-regex	Host name as a regular expression.	string	Maximum length: 255	
path	URL path as a regular expression.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default																		
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																		
	<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.																					
post-arg	Enable/disable use of body in the HTTP POST to match the query.	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.																					
category <id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295																			
url-list	External or Web filter URL list.	string	Maximum length: 35																			
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></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.			
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.																					
ua	Names of browsers to be used as user agent.	option	-																			

Parameter	Description	Type	Size	Default																
	<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-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																	
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																	
header-name	Name of HTTP header.	string	Maximum length: 79																	
header	HTTP header name as a regular expression.	string	Maximum length: 255																	
case-sensitivity	Enable to make the pattern case sensitive.	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.																			
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																	

Parameter	Description	Type	Size	Default
application <name>	SaaS application. SaaS application name.	string	Maximum length: 79	

config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	disable	Case insensitive in pattern.		
	enable	Case sensitive in pattern.		

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	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 type [src|dst]
set uuid {uuid}
set member <name1>, <name2>, ...
set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set comment {var-string}
next
end

```

config firewall proxy-addrgrp

Parameter	Description	Type	Size	Default
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
member <name>	Members of address group. Address name.	string	Maximum length: 79	
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	

config tagging

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

config firewall proxy-addrgrp6

Configure web proxy address group6.

```
config firewall proxy-addrgrp6
  Description: Configure web proxy address group6.
  edit <name>
    set type [src|dst]
    set uuid {uuid}
    set member <name1>, <name2>, ...
    set color {integer}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set comment {var-string}
  next
end
```

config firewall proxy-addrgrp6

Parameter	Description	Type	Size	Default
name	Address group6.	string	Maximum length: 79	
type	Source or destination address group6 type.	option	-	src
		Option	Description	
		src	Source group.	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dst</i>	Destination group.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
member <name>	Members of address group6. Address name.	string	Maximum length: 79	
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	

config tagging

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

config firewall region

Define region table.

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

config firewall region

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

config firewall response-shaping-policy

Configure HTTP response matching shaping policies.

```
config firewall response-shaping-policy
  Description: Configure HTTP response matching shaping policies.
  edit <id>
    set uuid {uuid}
    set name {string}
    set schedule {string}
    set comment {var-string}
    set status [enable|disable]
    set ip-version [4|6]
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set traffic-shaper {string}
    set traffic-shaper-reverse {string}
    set per-ip-shaper {string}
    set class-id {integer}
    set class-id-reverse {integer}
  next
end
```

config firewall response-shaping-policy

Parameter	Description	Type	Size	Default						
id	Response shaping policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
name	Response shaping policy name.	string	Maximum length: 35							
schedule	Schedule name.	string	Maximum length: 35	always						
comment	Comments.	var-string	Maximum length: 255							
status	Enable/disable response traffic shaping policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable traffic shaping policy.</td></tr><tr><td><i>disable</i></td><td>Disable traffic shaping policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable traffic shaping policy.	<i>disable</i>	Disable traffic shaping policy.
Option	Description									
<i>enable</i>	Enable traffic shaping policy.									
<i>disable</i>	Disable traffic shaping policy.									
ip-version	IP version.	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.									
srcaddr <name>	Source address. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address. Address name.	string	Maximum length: 79							
dstaddr6 <name>	IPv6 destination address. Address name.	string	Maximum length: 79							
traffic-shaper	Forward traffic shaper.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35	
per-ip-shaper	Per IP shaper.	string	Maximum length: 35	
class-id	Forward class id.	integer	Minimum value: 2 Maximum value: 31	0
class-id-reverse	Reverse class id.	integer	Minimum value: 2 Maximum value: 31	0

config firewall schedule group

Schedule group configuration.

```

config firewall schedule group
    Description: Schedule group configuration.
    edit <name>
        set member <name1>, <name2>, ...
        set color {integer}
        set fabric-object [enable|disable]
    next
end

```

config firewall schedule group

Parameter	Description	Type	Size	Default
name	Schedule group name.	string	Maximum length: 31	
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
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.		

config firewall schedule onetime

Onetime schedule configuration.

```
config firewall schedule onetime
  Description: Onetime schedule configuration.
  edit <name>
    set start {user}
    set start-utc {user}
    set end {user}
    set end-utc {user}
    set color {integer}
    set expiration-days {integer}
    set fabric-object [enable|disable]
  next
end
```

config firewall schedule onetime

Parameter	Description	Type	Size	Default
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	
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	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

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
	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.		

config firewall schedule recurring

Recurring schedule configuration.

```
config firewall schedule recurring
  Description: Recurring schedule configuration.
  edit <name>
    set start {user}
    set end {user}
    set day {option1}, {option2}, ...
    set color {integer}
    set fabric-object [enable|disable]
  next
end
```

config firewall schedule recurring

Parameter	Description	Type	Size	Default
name	Recurring schedule name.	string	Maximum length: 31	
start	Time of day to start the schedule, format hh:mm.	user	Not Specified	
end	Time of day to end the schedule, format hh:mm.	user	Not Specified	
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

Parameter	Description	Type	Size	Default																			
	<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.																						
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0																			
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.																						

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]
    next
end

```

config firewall service category

Parameter	Description	Type	Size	Default						
name	Service category name.	string	Maximum length: 63							
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.									

config firewall service custom

Configure custom services.

```
config firewall service custom
  Description: Configure custom services.
  edit <name>
    set proxy [enable|disable]
    set category {string}
    set protocol [TCP/UDP/SCTP/ICMP|...]
    set iprange {user}
    set fqdn {string}
    set protocol-number {integer}
    set icmptype {integer}
    set icmpcode {integer}
    set tcp-portrange {user}
    set udp-portrange {user}
    set sctp-portrange {user}
    set tcp-halfclose-timer {integer}
    set tcp-halfopen-timer {integer}
    set tcp-timewait-timer {integer}
    set tcp-rst-timer {integer}
    set udp-idle-timer {integer}
    set session-ttl {user}
    set check-reset-range [disable|strict|...]
    set comment {var-string}
    set color {integer}
    set app-service-type [disable|app-id|...]
    set app-category <id1>, <id2>, ...
    set application <id1>, <id2>, ...
    set fabric-object [enable|disable]
```



```
next
end
```

config firewall service custom

Parameter	Description	Type	Size	Default																						
name	Custom service name.	string	Maximum length: 79																							
proxy	Enable/disable web proxy service.	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.																									
category	Service category.	string	Maximum length: 63																							
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TCP/UDP/SCTP</i></td><td>TCP, UDP and SCTP.</td></tr><tr><td><i>ICMP</i></td><td>ICMP.</td></tr><tr><td><i>ICMP6</i></td><td>ICMP6.</td></tr><tr><td><i>IP</i></td><td>IP.</td></tr><tr><td><i>HTTP</i></td><td>HTTP - for web proxy.</td></tr><tr><td><i>FTP</i></td><td>FTP - for web proxy.</td></tr><tr><td><i>CONNECT</i></td><td>Connect - for web proxy.</td></tr><tr><td><i>SOCKS-TCP</i></td><td>Socks TCP - for web proxy.</td></tr><tr><td><i>SOCKS-UDP</i></td><td>Socks UDP - for web proxy.</td></tr><tr><td><i>ALL</i></td><td>All - for web proxy.</td></tr></table>				Option	Description	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.	<i>ICMP</i>	ICMP.	<i>ICMP6</i>	ICMP6.	<i>IP</i>	IP.	<i>HTTP</i>	HTTP - for web proxy.	<i>FTP</i>	FTP - for web proxy.	<i>CONNECT</i>	Connect - for web proxy.	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.	<i>SOCKS-UDP</i>	Socks UDP - for web proxy.	<i>ALL</i>	All - for web proxy.
	Option	Description																								
	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.																								
	<i>ICMP</i>	ICMP.																								
	<i>ICMP6</i>	ICMP6.																								
	<i>IP</i>	IP.																								
	<i>HTTP</i>	HTTP - for web proxy.																								
	<i>FTP</i>	FTP - for web proxy.																								
	<i>CONNECT</i>	Connect - for web proxy.																								
	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.																								
<i>SOCKS-UDP</i>	Socks UDP - for web proxy.																									
<i>ALL</i>	All - for web proxy.																									
iprange	Start and end of the IP range associated with service.	user	Not Specified																							
fqdn	Fully qualified domain name.	string	Maximum length: 255																							

Parameter	Description	Type	Size	Default
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295	
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255	
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
udp-portrange	Multiple UDP port ranges.	user	Not Specified	
sctp-portrange	Multiple SCTP port ranges.	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	0
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	0
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	0
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	0
udp-idle-timer	Number of seconds before an idle UDP connection times out (0 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400	0

Parameter	Description	Type	Size	Default								
session-ttl	Session TTL (300 - 2764800, 0 = default).	user	Not Specified									
check-reset-range	Configure the type of ICMP error message verification.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable RST range check.</td></tr><tr><td><i>strict</i></td><td>Check RST range strictly.</td></tr><tr><td><i>default</i></td><td>Using system default setting.</td></tr></table>				Option	Description	<i>disable</i>	Disable RST range check.	<i>strict</i>	Check RST range strictly.	<i>default</i>	Using system default setting.
	Option	Description										
	<i>disable</i>	Disable RST range check.										
	<i>strict</i>	Check RST range strictly.										
<i>default</i>	Using system default setting.											
comment	Comment.	var-string	Maximum length: 255									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0								
app-service-type	Application service type.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable application type.</td></tr><tr><td><i>app-id</i></td><td>Application ID.</td></tr><tr><td><i>app-category</i></td><td>Applicatin category.</td></tr></table>				Option	Description	<i>disable</i>	Disable application type.	<i>app-id</i>	Application ID.	<i>app-category</i>	Applicatin category.
	Option	Description										
	<i>disable</i>	Disable application type.										
	<i>app-id</i>	Application ID.										
<i>app-category</i>	Applicatin category.											
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295									
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295									
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.											

config firewall service group

Configure service groups.

```
config firewall service group
  Description: Configure service groups.
  edit <name>
    set proxy [enable|disable]
    set member <name1>, <name2>, ...
    set comment {var-string}
    set color {integer}
    set fabric-object [enable|disable]
  next
end
```

config firewall service group

Parameter	Description	Type	Size	Default						
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><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.									
member <name>	Service objects contained within the group. Service or service group name.	string	Maximum length: 79							
comment	Comment.	var-string	Maximum length: 255							
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
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.									

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 max-bandwidth {integer}
    set bandwidth-unit [kbps|mbps|...]
    set max-concurrent-session {integer}
    set max-concurrent-tcp-session {integer}
    set max-concurrent-udp-session {integer}
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
  next
end
```

config firewall shaper per-ip-shaper

Parameter	Description	Type	Size	Default								
name	Traffic shaper name.	string	Maximum length: 35									
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								
bandwidth-unit	Unit of measurement for 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.											
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								

Parameter	Description	Type	Size	Default						
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						
diffserv-forward	Enable/disable changing the Forward (original) 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 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/disable changing the Reverse (reply) 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 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	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							

config firewall shaper traffic-shaper

Configure shared traffic shaper.

```
config firewall shaper traffic-shaper
  Description: Configure shared traffic shaper.
  edit <name>
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
    set bandwidth-unit [kbps|mbps|...]
    set priority [low|medium|...]
    set per-policy [disable|enable]
```

```

set diffserv [enable|disable]
set diffservcode {user}
set dscp-marking-method [multi-stage|static]
set exceed-bandwidth {integer}
set exceed-dscp {user}
set maximum-dscp {user}
set overhead {integer}
next
end

```

config firewall shaper traffic-shaper

Parameter	Description	Type	Size	Default								
name	Traffic shaper name.	string	Maximum length: 35									
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper (0 - 800000000). Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 800000000	0								
maximum-bandwidth	Upper bandwidth limit enforced by this shaper (0 - 800000000). 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 800000000	0								
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><i>kbps</i></td><td>Kilobits per second.</td></tr><tr><td><i>mbps</i></td><td>Megabits per second.</td></tr><tr><td><i>gbps</i></td><td>Gigabits per second.</td></tr></table>				Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.
Option	Description											
<i>kbps</i>	Kilobits per second.											
<i>mbps</i>	Megabits per second.											
<i>gbps</i>	Gigabits per second.											
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Low priority.</td></tr><tr><td><i>medium</i></td><td>Medium priority.</td></tr><tr><td><i>high</i></td><td>High priority.</td></tr></table>				Option	Description	<i>low</i>	Low priority.	<i>medium</i>	Medium priority.	<i>high</i>	High priority.
Option	Description											
<i>low</i>	Low priority.											
<i>medium</i>	Medium priority.											
<i>high</i>	High priority.											

Parameter	Description	Type	Size	Default
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
	Option	Description		
	<i>disable</i>	All referring policies share one traffic shaper.		
	<i>enable</i>	Each referring policy has its own traffic shaper.		
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting traffic DiffServ.		
	<i>disable</i>	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
	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 Maximum value: 80000000	0
exceed-dscp	DSCP mark for traffic in guaranteed-bandwidth and exceed-bandwidth.	user	Not Specified	
maximum-dscp	DSCP mark for traffic in exceed-bandwidth and maximum-bandwidth.	user	Not Specified	
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 Maximum value: 100	0

config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
  Description: Configure shaping policies.
  edit <id>
    set uuid {uuid}
    set name {string}
    set comment {var-string}
    set status [enable|disable]
    set ip-version [4|6]
    set service-type [service|internet-service]
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    set internet-service-name <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set schedule {string}
    set http-response-match [enable|disable]
    set users <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set traffic-shaper {string}
    set traffic-shaper-reverse {string}
    set per-ip-shaper {string}
    set class-id {integer}
    set class-id-reverse {integer}
    set diffserv-forward [enable|disable]
    set diffservcode-forward {user}
    set diffserv-reverse [enable|disable]
    set diffservcode-rev {user}
  next
end
```

config firewall shaping-policy

Parameter	Description	Type	Size	Default						
id	Shaping policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
name	Shaping policy name.	string	Maximum length: 35							
comment	Comments.	var-string	Maximum length: 255							
status	Enable/disable traffic shaping policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable traffic shaping policy.</td></tr><tr><td><i>disable</i></td><td>Disable traffic shaping policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable traffic shaping policy.	<i>disable</i>	Disable traffic shaping policy.
Option	Description									
<i>enable</i>	Enable traffic shaping policy.									
<i>disable</i>	Disable traffic shaping policy.									
ip-version	IP version.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>4</i></td><td>Use IPv4 addressing for Configuration Method.</td></tr><tr><td><i>6</i></td><td>Use IPv6 addressing for Configuration Method.</td></tr></table>				Option	Description	<i>4</i>	Use IPv4 addressing for Configuration Method.	<i>6</i>	Use IPv6 addressing for Configuration Method.
Option	Description									
<i>4</i>	Use IPv4 addressing for Configuration Method.									
<i>6</i>	Use IPv6 addressing for Configuration Method.									
service-type	Select service-type: service / internet-service.	option	-	service						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>service</i></td><td>Firewall services.</td></tr><tr><td><i>internet-service</i></td><td>Internet-services.</td></tr></table>				Option	Description	<i>service</i>	Firewall services.	<i>internet-service</i>	Internet-services.
Option	Description									
<i>service</i>	Firewall services.									
<i>internet-service</i>	Internet-services.									
srcaddr <name>	Source address. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address. Address name.	string	Maximum length: 79							
srcaddr6 <name>	IPv6 source address. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
dstaddr6 <name>	IPv6 destination address. Address name.	string	Maximum length: 79							
service <name>	Service name. Service name.	string	Maximum length: 79							
internet- service-name <name>	Internet Service ID. Internet Service name.	string	Maximum length: 79							
internet- service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
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							
schedule	Schedule name.	string	Maximum length: 35	always						
http-response- match	Enable/disable matching http response shaping policies.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable matching HTTP response shaping policies.</td></tr><tr><td><i>disable</i></td><td>Disable matching HTTP response shaping policies.</td></tr></table>				Option	Description	<i>enable</i>	Enable matching HTTP response shaping policies.	<i>disable</i>	Disable matching HTTP response shaping policies.
Option	Description									
<i>enable</i>	Enable matching HTTP response shaping policies.									
<i>disable</i>	Disable matching HTTP response shaping policies.									
users <name>	User name. User name.	string	Maximum length: 79							
groups <name>	User authentication groups. 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							
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to.	integer	Minimum value: 0 Maximum value: 4294967295							

Parameter	Description	Type	Size	Default						
	Category IDs.									
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79							
dstintf <name>	Destination interface list. Interface name.	string	Maximum length: 79							
traffic-shaper	Forward traffic shaper.	string	Maximum length: 35							
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35							
per-ip-shaper	Per IP shaper.	string	Maximum length: 35							
class-id	Forward class id.	integer	Minimum value: 2 Maximum value: 31	0						
class-id-reverse	Reverse class id.	integer	Minimum value: 2 Maximum value: 31	0						
diffserv-forward	Enable/disable forward (original) traffic DiffServ.	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-forward	Forward (original) traffic DiffServ code point value.	user	Not Specified							
diffserv-reverse	Enable/disable reverse (reply) traffic DiffServ.	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-rev	Reverse (reply) traffic DiffServ code point value.	user	Not Specified							

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 {integer}
    config classes
      Description: Define shaping classes of this shaping profile
      edit <name>
        set class-id {integer}
        set priority [top|critical|...]
        set guaranteed-bandwidth {integer}
        set maximum-bandwidth {integer}
      next
    end
    set npu-offloading [disable|enable]
  next
end
```

config firewall shaping-profile

Parameter	Description	Type	Size	Default
profile-name	Shaping profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 1023	
default-class	Default class ID to handle unclassified packets.	integer	Minimum value: 2 Maximum value: 32	2
npu-offloading	Enable/disable NPU offloading.	option	-	enable
		Option	Description	
		<i>disable</i>	Disable shaper offloading.	
		<i>enable</i>	Enable shaper offloading.	

config classes

Parameter	Description	Type	Size	Default
name	Class Name.	string	Maximum length: 35	
class-id	Class ID.	integer	Minimum value: 2 Maximum value: 32	0
priority	Priority.	option	-	top
	Option	Description		
	<i>top</i>	Top priority.		
	<i>critical</i>	Critical priority.		
	<i>high</i>	High priority.		
	<i>medium</i>	Medium priority.		
	<i>low</i>	Low priority.		
guaranteed-bandwidth	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100	0
maximum-bandwidth	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1

config firewall sniffer

Configure sniffer.

```
config firewall sniffer
  Description: Configure sniffer.
  edit <id>
    set uuid {uuid}
    set status [enable|disable]
    set logtraffic [all|utm|...]
    set non-ip [enable|disable]
    set interface {string}
    set host {string}
    set port {string}
    set protocol {string}
    set vlan {string}
```

```
next
end
```

config firewall sniffer

Parameter	Description	Type	Size	Default								
id	Sniffer ID (0 - 9999).	integer	Minimum value: 0 Maximum value: 9999	0								
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000								
status	Enable/disable the active status of the sniffer.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer status.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer status.</td></tr></table>				Option	Description	<i>enable</i>	Enable sniffer status.	<i>disable</i>	Disable sniffer status.		
Option	Description											
<i>enable</i>	Enable sniffer status.											
<i>disable</i>	Disable sniffer status.											
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	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.											
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer for non-IP packets.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer for non-IP packets.</td></tr></table>				Option	Description	<i>enable</i>	Enable sniffer for non-IP packets.	<i>disable</i>	Disable sniffer for non-IP packets.		
Option	Description											
<i>enable</i>	Enable sniffer for non-IP packets.											
<i>disable</i>	Disable sniffer for non-IP packets.											
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default
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	
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	
vlan	List of VLANs to sniff.	string	Maximum length: 63	

config firewall ssh host-key

SSH proxy host public keys.

```

config firewall ssh host-key
    Description: SSH proxy host public keys.
    edit <name>
        set status [trusted|revoked]
        set type [RSA|DSA|...]
        set nid [256|384|...]
        set usage [transparent-proxy|access-proxy]
        set ip {ipv4-address-any}
        set port {integer}
        set hostname {string}
        set public-key {var-string}
    next
end

```

config firewall ssh host-key

Parameter	Description	Type	Size	Default
name	SSH public key name.	string	Maximum length: 35	
status	Set the trust status of the public key.	option	-	trusted
	Option	Description		
	<i>trusted</i>	The public key is trusted.		
	<i>revoked</i>	The public key is revoked.		
type	Set the type of the public key.	option	-	RSA

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>RSA</i></td><td>The type of the public key is RSA.</td></tr><tr><td><i>DSA</i></td><td>The type of the public key is DSA.</td></tr><tr><td><i>ECDSA</i></td><td>The type of the public key is ECDSA.</td></tr><tr><td><i>ED25519</i></td><td>The type of the public key is ED25519.</td></tr><tr><td><i>RSA-CA</i></td><td>The type of the public key is from RSA CA.</td></tr><tr><td><i>DSA-CA</i></td><td>The type of the public key is from DSA CA.</td></tr><tr><td><i>ECDSA-CA</i></td><td>The type of the public key is from ECDSA CA.</td></tr><tr><td><i>ED25519-CA</i></td><td>The type of the public key is from ED25519 CA.</td></tr></table>	Option	Description	<i>RSA</i>	The type of the public key is RSA.	<i>DSA</i>	The type of the public key is DSA.	<i>ECDSA</i>	The type of the public key is ECDSA.	<i>ED25519</i>	The type of the public key is ED25519.	<i>RSA-CA</i>	The type of the public key is from RSA CA.	<i>DSA-CA</i>	The type of the public key is from DSA CA.	<i>ECDSA-CA</i>	The type of the public key is from ECDSA CA.	<i>ED25519-CA</i>	The type of the public key is from ED25519 CA.			
	Option	Description																				
	<i>RSA</i>	The type of the public key is RSA.																				
	<i>DSA</i>	The type of the public key is DSA.																				
	<i>ECDSA</i>	The type of the public key is ECDSA.																				
	<i>ED25519</i>	The type of the public key is ED25519.																				
	<i>RSA-CA</i>	The type of the public key is from RSA CA.																				
	<i>DSA-CA</i>	The type of the public key is from DSA CA.																				
	<i>ECDSA-CA</i>	The type of the public key is from ECDSA CA.																				
<i>ED25519-CA</i>	The type of the public key is from ED25519 CA.																					
nid	Set the nid of the ECDSA key.	option	-	256																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>256</i></td><td>The NID is ecdsa-sha2-nistp256.</td></tr><tr><td><i>384</i></td><td>The NID is ecdsa-sha2-nistp384.</td></tr><tr><td><i>521</i></td><td>The NID is ecdsa-sha2-nistp521.</td></tr></table>	Option	Description	<i>256</i>	The NID is ecdsa-sha2-nistp256.	<i>384</i>	The NID is ecdsa-sha2-nistp384.	<i>521</i>	The NID is ecdsa-sha2-nistp521.													
	Option	Description																				
	<i>256</i>	The NID is ecdsa-sha2-nistp256.																				
	<i>384</i>	The NID is ecdsa-sha2-nistp384.																				
<i>521</i>	The NID is ecdsa-sha2-nistp521.																					
usage	Usage for this public key.	option	-	transparent-proxy																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>transparent-proxy</i></td><td>Transparent proxy uses this public key to validate server.</td></tr><tr><td><i>access-proxy</i></td><td>Access proxy uses this public key to validate server.</td></tr></table>	Option	Description	<i>transparent-proxy</i>	Transparent proxy uses this public key to validate server.	<i>access-proxy</i>	Access proxy uses this public key to validate server.															
	Option	Description																				
	<i>transparent-proxy</i>	Transparent proxy uses this public key to validate server.																				
<i>access-proxy</i>	Access proxy uses this public key to validate server.																					
ip	IP address of the SSH server.	ipv4-address-any	Not Specified	0.0.0.0																		
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295	22																		
hostname	Hostname of the SSH server to match SSH certificate principals.	string	Maximum length: 255																			
public-key	SSH public key.	var-string	Maximum length: 32768																			

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	
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
		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 untrusted-caname {string}
  set hostkey-rsa2048 {string}
  set hostkey-dsa1024 {string}
  set hostkey-ecdsa256 {string}
  set hostkey-ecdsa384 {string}
  set hostkey-ecdsa521 {string}
  set hostkey-ed25519 {string}
  set host-trusted-checking [enable|disable]
end
```

config firewall ssh setting

Parameter	Description	Type	Size	Default
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35	
untrusted-caname	Untrusted CA certificate used by SSH Inspection.	string	Maximum length: 35	
hostkey-rsa2048	RSA certificate used by SSH proxy.	string	Maximum length: 35	
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	
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	
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.	

config firewall ssl default-certificate

SSL default certificate.

```
config firewall ssl default-certificate
  Description: SSL default certificate.
  set default-ca {string}
  set default-untrusted-ca {string}
  set default-server-cert {string}
end
```

config firewall ssl default-certificate

Parameter	Description	Type	Size	Default
default-ca	Default CA certificate used by SSL inspection.	string	Maximum length: 35	Fortinet_CA_SSL
default-untrusted-ca	Default CA certificate used by SSL inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted
default-server-cert	Default server certificate used by SSL inspection.	string	Maximum length: 35	Fortinet_Factory

config firewall ssl keyring-list

SSL keyring list.

```
config firewall ssl keyring-list
  Description: SSL keyring list.
  edit <name>
    set uuid {uuid}
  next
end
```

config firewall ssl keyring-list

Parameter	Description	Type	Size	Default
name	Keyring list name.	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 firewall ssl setting

SSL proxy settings.

```
config firewall ssl setting
  Description: SSL proxy settings.
  set proxy-connect-timeout {integer}
  set ssl-dh-bits [768|1024|...]
  set ssl-send-empty-frags [enable|disable]
  set no-matching-cipher-action [bypass|drop]
```

```

set cert-manager-cache-timeout {integer}
set resigned-short-lived-certificate [enable|disable]
set cert-cache-capacity {integer}
set cert-cache-timeout {integer}
set session-cache-capacity {integer}
set session-cache-timeout {integer}
set abbreviate-handshake [enable|disable]
end

```

config firewall ssl setting

Parameter	Description	Type	Size	Default										
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										
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>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></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.			
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-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										
	<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.													
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.													

Parameter	Description	Type	Size	Default						
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						
resigned-short-lived-certificate	Enable/disable short-lived certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></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><i>disable</i></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	<i>enable</i>	Enable short-lived certificate: re-signed certificate will remain valid until either the origin server certificate expires or cache timeouts.	<i>disable</i>	Disable short-lived certificate: re-signed certificate will have the same validation period as the origin server certificate.			
Option	Description									
<i>enable</i>	Enable short-lived certificate: re-signed certificate will remain valid until either the origin server certificate expires or cache timeouts.									
<i>disable</i>	Disable short-lived certificate: re-signed certificate will have the same validation period as the origin server certificate.									
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						
session-cache-capacity	Capacity of the SSL session cache (-- Obsolete--) (1 - 1000, default = 500).	integer	Minimum value: 0 Maximum value: 1000	500						
session-cache-timeout	Time limit to keep SSL session state (1 - 60 min, default = 20).	integer	Minimum value: 1 Maximum value: 60	20						
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of SSL abbreviated handshake.</td></tr><tr><td><i>disable</i></td><td>Disable use of SSL abbreviated handshake.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of SSL abbreviated handshake.	<i>disable</i>	Disable use of SSL abbreviated handshake.			
Option	Description									
<i>enable</i>	Enable use of SSL abbreviated handshake.									
<i>disable</i>	Disable use of SSL abbreviated handshake.									

config firewall ssl-server

Configure SSL servers.

```

config firewall ssl-server
    Description: Configure SSL servers.
    edit <name>
        set ip {ipv4-address-any}
        set port {integer}
        set ssl-mode [half|full]
        set add-header-x-forwarded-proto [enable|disable]
        set mapped-port {integer}
        set ssl-cert <name1>, <name2>, ...
        set ssl-dh-bits [768|1024|...]
        set ssl-algorithm [high|medium|...]
        set ssl-client-renegotiation [allow|deny|...]
        set ssl-min-version [tls-1.0|tls-1.1|...]
        set ssl-max-version [tls-1.0|tls-1.1|...]
        set ssl-send-empty-frags [enable|disable]
        set url-rewrite [enable|disable]
    next
end

```

config firewall ssl-server

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 35	
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
port	Server service port (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	443
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full
	Option	Description		
	half	Client to FortiProxy SSL.		
	full	Client to FortiProxy and FortiProxy to Server SSL.		
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add X-Forwarded-Proto header.</td></tr><tr><td><i>disable</i></td><td>Do not add X-Forwarded-Proto header.</td></tr></table>	Option	Description	<i>enable</i>	Add X-Forwarded-Proto header.	<i>disable</i>	Do not add X-Forwarded-Proto header.							
	Option	Description												
	<i>enable</i>	Add X-Forwarded-Proto header.												
<i>disable</i>	Do not add X-Forwarded-Proto header.													
mapped-port	Mapped server service port (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535	80										
ssl-cert <name>	List of certificate names to use for SSL connections to this server. (default = "Fortinet_SSL"). 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.													
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-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.													

Parameter	Description	Type	Size	Default
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1
	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-max-version	Highest SSL/TLS version to negotiate.	option	-	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-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 comment {var-string}
  config ssl
```

```

Description: Configure SSL options.
set inspect-all [disable|certificate-inspection|...]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-version [allow|block]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
set cert-probe-failure [allow|block]
set encrypted-client-hello [allow|block]
set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
config https
Description: Configure HTTPS options.
set ports {integer}
set status [disable|certificate-inspection|...]
set quic [inspect|bypass|...]
set proxy-after-tcp-handshake [enable|disable]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-version [allow|block]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
set cert-probe-failure [allow|block]
set encrypted-client-hello [allow|block]
set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
config ftps
Description: Configure FTPS options.
set ports {integer}
set status [disable|deep-inspection]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-version [allow|block]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end

```

```

config imaps
    Description: Configure IMAPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config pop3s
    Description: Configure POP3S options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config smtps
    Description: Configure SMTPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ssh
    Description: Configure SSH options.
    set ports {integer}
    set status [disable|deep-inspection]

```

```

    set inspect-all [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set unsupported-version [bypass|block]
    set ssh-tun-policy-check [disable|enable]
    set ssh-algorithm [compatible|high-encryption]
end
config dot
    Description: Configure DNS over TLS options.
    set status [disable|deep-inspection]
    set quic [inspect|bypass|...]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ssl-client-certificate
    Description: Configure SSL client certificate setting.
    set status [do-not-offer|keyring-list|...]
    set keyring-list {string}
    set caname {string}
    set cert {string}
end
config ssl-exempt
    Description: Servers to exempt from SSL inspection.
    edit <id>
        set type [fortiguard-category|address|...]
        set fortiguard-category {integer}
        set address {string}
        set address6 {string}
        set wildcard-fqdn {string}
        set regex {string}
        set finger-print-category [unknown|firefox|...]
    next
end
config ech-outer-sni
    Description: ClientHelloOuter SNIs to be blocked.
    edit <name>
        set sni {string}
    next
end
set allowlist [enable|disable]
set block-blocklisted-certificates [disable|enable]
set server-cert-mode [re-sign|replace]
set use-ssl-server [disable|enable]
set caname {string}

```

```

set untrusted-caname {string}
set server-cert <name1>, <name2>, ...
config ssl-server
    Description: SSL server settings used for client certificate request.
    edit <id>
        set ip {ipv4-address-any}
        set https-client-certificate [bypass|inspect|...]
        set smtps-client-certificate [bypass|inspect|...]
        set pop3s-client-certificate [bypass|inspect|...]
        set imaps-client-certificate [bypass|inspect|...]
        set ftps-client-certificate [bypass|inspect|...]
        set ssl-other-client-certificate [bypass|inspect|...]
    next
end
set ssl-exemption-ip-rating [enable|disable]
set ssl-exemption-log [disable|enable]
set ssl-anomaly-log [disable|enable]
set ssl-negotiation-log [disable|enable]
set ssl-server-cert-log [disable|enable]
set ssl-handshake-log [disable|enable]
set rpc-over-https [enable|disable]
set mapi-over-https [enable|disable]
set supported-alpn [http1-1|http2|...]
next
end

```

config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 35							
comment	Optional comments.	var-string	Maximum length: 255							
allowlist	Enable/disable exempting servers by FortiGuard allowlist.	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.									
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blacklist.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable FortiGuard certificate blocklist.		
	<i>enable</i>	Enable FortiGuard certificate blocklist.		
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign
	Option	Description		
	<i>re-sign</i>	Multiple clients connecting to multiple servers.		
	<i>replace</i>	Protect an SSL server.		
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.		
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	default-ca
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	default-untrusted-ca
server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 79	
ssl-exemption-ip-rating	Enable/disable IP based URL rating.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IP based URL rating.		
	<i>disable</i>	Disable IP based URL rating.		
ssl-exemption-log	Enable/disable logging of SSL exemptions.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging of SSL exemptions.		
	<i>enable</i>	Enable logging of SSL exemptions.		
ssl-anomaly-log	Enable/disable logging of SSL anomalies.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging of SSL anomalies.		
	<i>enable</i>	Enable logging of SSL anomalies.		
ssl-negotiation-log	Enable/disable logging of SSL negotiation events.	option	-	enable
	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.		
ssl-handshake-log	Enable/disable logging of TLS handshakes.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of TLS handshakes.		
	<i>enable</i>	Enable logging of TLS handshakes.		
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.		

Parameter	Description	Type	Size	Default										
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of MAPI over HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of MAPI over HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable inspection of MAPI over HTTPS.	<i>disable</i>	Disable inspection of MAPI over HTTPS.							
Option	Description													
<i>enable</i>	Enable inspection of MAPI over HTTPS.													
<i>disable</i>	Disable inspection of MAPI over HTTPS.													
supported-alpn	Configure ALPN option.	option	-	all										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http1-1</i></td><td>Enable all ALPN including HTTP1.1 except HTTP2 and SPDY.</td></tr><tr><td><i>http2</i></td><td>Enable all ALPN including HTTP2 except HTTP1.1 and SPDY.</td></tr><tr><td><i>all</i></td><td>Allow all ALPN extensions except SPDY.</td></tr><tr><td><i>none</i></td><td>Do not use ALPN.</td></tr></table>	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.			
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.													

config ssl

Parameter	Description	Type	Size	Default										
inspect-all	Level of SSL inspection.	option	-	disable										
	<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.													
client-certificate	Action based on received client certificate.	option	-	bypass										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></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><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
	Option	Description												
	<i>bypass</i>	Bypass the session.												
	<i>inspect</i>	Inspect the session.												
	<i>block</i>	Block the session.												
<i>bypass-on-cert-req</i>	Bypass on certificate request.													

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.											
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.											
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.											
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.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								

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.		
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.		
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
	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.		
cert-probe-failure	Action based on certificate probe failure.	option	-	block

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when unable to retrieve server's certificate for inspection.</td></tr><tr><td><i>block</i></td><td>Block the session when unable to retrieve server's certificate for inspection.</td></tr></table>	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.									
	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.															
encrypted-client-hello	Block/allow session based on existence of encrypted-client-hello.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Pass the session when encrypted-client-hello exists.</td></tr><tr><td><i>block</i></td><td>Block the session when encrypted-client-hello exists.</td></tr></table>	Option	Description	<i>allow</i>	Pass the session when encrypted-client-hello exists.	<i>block</i>	Block the session when encrypted-client-hello exists.									
	Option	Description														
	<i>allow</i>	Pass the session when encrypted-client-hello exists.														
<i>block</i>	Block the session when encrypted-client-hello exists.															
min-allowed-ssl-version	Minimum SSL version to be allowed.	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.															

config https

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	Option	Description		
	disable	Disable.		
	certificate-inspection	Inspect SSL handshake only.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>deep-inspection</i>	Full SSL inspection.									
	Option	Description												
<i>deep-inspection</i>	Full SSL inspection.													
quic	QUIC inspection status (default = inspect).	option	-	inspect										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inspect</i></td><td>Inspect QUIC traffic.</td></tr><tr><td><i>bypass</i></td><td>Bypass QUIC traffic.</td></tr><tr><td><i>block</i></td><td>Block QUIC traffic.</td></tr></table>	Option	Description	<i>inspect</i>	Inspect QUIC traffic.	<i>bypass</i>	Bypass QUIC traffic.	<i>block</i>	Block QUIC traffic.					
	Option	Description												
	<i>inspect</i>	Inspect QUIC traffic.												
	<i>bypass</i>	Bypass QUIC traffic.												
<i>block</i>	Block QUIC traffic.													
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.													
client-certificate	Action based on received client certificate.	option	-	bypass										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></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><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
	Option	Description												
	<i>bypass</i>	Bypass the session.												
	<i>inspect</i>	Inspect the session.												
	<i>block</i>	Block the session.												
<i>bypass-on-cert-req</i>	Bypass on certificate request.													
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.													
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.		
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.		
revoked-server-cert	Action based on server certificate is revoked.	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.		
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.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

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-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.		
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
	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.		
cert-probe-failure	Action based on certificate probe failure.	option	-	block
	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.		
encrypted-client-hello	Block/allow session based on existence of encrypted-client-hello.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Pass the session when encrypted-client-hello exists.		
	<i>block</i>	Block the session when encrypted-client-hello exists.		
min-allowed-ssl-version	Minimum SSL version to be allowed.	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.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config ftps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bypass-on-cert-req</i>	Bypass on certificate request.		
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.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	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.		
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.		
revoked-server-cert	Action based on server certificate is revoked.	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								
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.											
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.											
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.											
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.											
min-allowed-ssl-version	Minimum SSL version to be allowed.	option	-	tls-1.1								

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 imaps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
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.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bypass-on-cert-req</i>	Bypass on certificate request.		
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.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	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.		
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.		
revoked-server-cert	Action based on server certificate is revoked.	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								
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.											
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.											
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.											
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.											

config pop3s

Parameter	Description	Type	Size	Default										
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535											
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.													
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.													
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><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
Option	Description													
<i>bypass</i>	Bypass the session.													
<i>inspect</i>	Inspect the session.													
<i>block</i>	Block the session.													
<i>bypass-on-cert-req</i>	Bypass on certificate request.													
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.													
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.		
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.		
revoked-server-cert	Action based on server certificate is revoked.	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.		
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.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

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-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.		
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
	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.		

config smtps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
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.		
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.		
	<i>bypass-on-cert-req</i>	Bypass on certificate request.		
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.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	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

Parameter	Description	Type	Size	Default
	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.		
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.		
revoked-server-cert	Action based on server certificate is revoked.	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.		
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.		
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.		
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.		
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
	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.		

config ssh

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
inspect-all	Level of SSL inspection.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		

Parameter	Description	Type	Size	Default						
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.									
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>block</i>	Block the session.			
Option	Description									
<i>bypass</i>	Bypass the session.									
<i>block</i>	Block the session.									
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSH tunnel policy check.</td></tr><tr><td><i>enable</i></td><td>Enable SSH tunnel policy check.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSH tunnel policy check.	<i>enable</i>	Enable SSH tunnel policy check.			
Option	Description									
<i>disable</i>	Disable SSH tunnel policy check.									
<i>enable</i>	Enable SSH tunnel policy check.									
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>compatible</i></td><td>Allow a broader set of encryption algorithms for best compatibility.</td></tr><tr><td><i>high-encryption</i></td><td>Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.</td></tr></table>	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.			
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.									

config dot

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		

Parameter	Description	Type	Size	Default										
quic	QUIC inspection status (default = inspect).	option	-	inspect										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inspect</i></td><td>Inspect QUIC traffic.</td></tr><tr><td><i>bypass</i></td><td>Bypass QUIC traffic.</td></tr><tr><td><i>block</i></td><td>Block QUIC traffic.</td></tr></table>	Option	Description	<i>inspect</i>	Inspect QUIC traffic.	<i>bypass</i>	Bypass QUIC traffic.	<i>block</i>	Block QUIC traffic.					
Option	Description													
<i>inspect</i>	Inspect QUIC traffic.													
<i>bypass</i>	Bypass QUIC traffic.													
<i>block</i>	Block QUIC traffic.													
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.													
client-certificate	Action based on received client certificate.	option	-	bypass										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></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><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
Option	Description													
<i>bypass</i>	Bypass the session.													
<i>inspect</i>	Inspect the session.													
<i>block</i>	Block the session.													
<i>bypass-on-cert-req</i>	Bypass on certificate request.													
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.													
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										

Parameter	Description	Type	Size	Default
	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.		
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.		
revoked-server-cert	Action based on server certificate is revoked.	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.		
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.		
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.		
cert-validation-failure	Action based on certificate validation failure.	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.											

config ssl-client-certificate

Parameter	Description	Type	Size	Default										
status	Configure SSL client certificate status.	option	-	do-not-offer										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>do-not-offer</i></td><td>Do not offer SSL client certificate.</td></tr><tr><td><i>keyring-list</i></td><td>For authenticated users, offer matching SSL client certificate from keyring list.</td></tr><tr><td><i>ca-sign</i></td><td>For authenticated users, offer SSL client certificate signed by configured CA.</td></tr><tr><td><i>static</i></td><td>Offer static SSL client certificate.</td></tr></table>	Option	Description	<i>do-not-offer</i>	Do not offer SSL client certificate.	<i>keyring-list</i>	For authenticated users, offer matching SSL client certificate from keyring list.	<i>ca-sign</i>	For authenticated users, offer SSL client certificate signed by configured CA.	<i>static</i>	Offer static SSL client certificate.			
	Option	Description												
	<i>do-not-offer</i>	Do not offer SSL client certificate.												
	<i>keyring-list</i>	For authenticated users, offer matching SSL client certificate from keyring list.												
	<i>ca-sign</i>	For authenticated users, offer SSL client certificate signed by configured CA.												
<i>static</i>	Offer static SSL client certificate.													
keyring-list	Keyring list used to find client certificate.	string	Maximum length: 35											
caname	CA certificate used to sign client certificate.	string	Maximum length: 35	Fortinet_CA_SSL										
cert	Client certificate.	string	Maximum length: 35											

config ssl-exempt

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 512	0
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-	fortiguard-category
	Option	Description		
	<i>fortiguard-category</i>	FortiGuard category.		
	<i>address</i>	Firewall IPv4 address.		
	<i>address6</i>	Firewall IPv6 address.		
	<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.		
	<i>regex</i>	Regular expression FQDN.		
	<i>finger-print</i>	TLS finger print.		
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0
address	IPv4 address object.	string	Maximum length: 79	
address6	IPv6 address object.	string	Maximum length: 79	
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79	
regex	Exempt servers by regular expression.	string	Maximum length: 255	
finger-print-category	Finger print platform.	option	-	android
	Option	Description		
	<i>unknown</i>	Unknown clients.		
	<i>firefox</i>	Firefox.		
	<i>chrome</i>	Chrome.		
	<i>safari</i>	Safari.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>edge</i>	Edge.		
	<i>ie</i>	Internet Explorer.		
	<i>android</i>	Android applications.		
	<i>ios</i>	iOS applications.		
	<i>windows</i>	Windows applications.		

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 ssl-server

Parameter	Description	Type	Size	Default
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	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 status [enable|disable]
    set action [accept|deny]
    set srcintf {string}
    set srcaddr <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    set schedule {string}
    set ttl {user}
  next
end
```

config firewall ttl-policy

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable this TTL policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this TTL policy.</td></tr><tr><td><i>disable</i></td><td>Disable this TTL policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable this TTL policy.	<i>disable</i>	Disable this TTL policy.			
	Option	Description								
	<i>enable</i>	Enable this TTL policy.								
<i>disable</i>	Disable this TTL policy.									
action	Action to be performed on traffic matching this policy (default = deny).	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Allow traffic matching this policy.</td></tr><tr><td><i>deny</i></td><td>Deny or block traffic matching this policy.</td></tr></table>	Option	Description	<i>accept</i>	Allow traffic matching this policy.	<i>deny</i>	Deny or block traffic matching this policy.			
	Option	Description								
	<i>accept</i>	Allow traffic matching this policy.								
<i>deny</i>	Deny or block traffic matching this policy.									
srcintf	Source interface name from available interfaces.	string	Maximum length: 35							
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79							
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79							
schedule	Schedule object from available options.	string	Maximum length: 35							
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.

```
config firewall vendor-mac
  Description: Show vendor and the MAC address they have.
```

```

edit <id>
    set name {string}
    set mac-number {integer}
    set obsolete {integer}
next
end

```

config firewall vendor-mac

Parameter	Description	Type	Size	Default
id	Vendor ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Vendor name.	string	Maximum length: 63	
mac-number	Total number of MAC addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0
obsolete	Indicates whether the Vendor ID can be used.	integer	Minimum value: 0 Maximum value: 255	0

config firewall vendor-mac-summary

Vendor MAC database summary.

```

config firewall vendor-mac-summary
    Description: Vendor MAC database summary.
end

```

config firewall vip

Configure virtual IP for IPv4.

```

config firewall vip
    Description: Configure virtual IP for IPv4.
    edit <name>

```

```

set id {integer}
set uuid {uuid}
set comment {var-string}
set type [static-nat|server-load-balance|...]
set server-type [http|https|...]
set ldb-method [static|round-robin|...]
set extip {user}
set h2-support [enable|disable]
set h3-support [enable|disable]
config quic
    Description: QUIC setting.
    set max-idle-timeout {integer}
    set max-udp-payload-size {integer}
    set active-connection-id-limit {integer}
    set ack-delay-exponent {integer}
    set max-ack-delay {integer}
    set max-datagram-frame-size {integer}
    set active-migration [enable|disable]
    set grease-quic-bit [enable|disable]
end
set mappedip <range1>, <range2>, ...
set extintf {string}
set arp-reply [disable|enable]
set http-redirect [enable|disable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set status [disable|enable]
set protocol [tcp|udp|...]
set extport {user}
set mappedport {user}
set gratuitous-arp-interval {integer}
set empty-cert-action [accept|block|...]
set user-agent-detect [disable|enable]
set client-cert [disable|enable]
config realservers
    Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
    edit <id>
        set type [ip|address]
        set address {string}
        set ip {user}
        set port {integer}
        set status [active|standby|...]
        set weight {integer}
        set holddown-interval {integer}
        set healthcheck [disable|enable]
        set health-check-proto [ping|http]
        set http-host {string}
        set translate-host [enable|disable]
        set max-connections {integer}
        set client-ip {user}
        set verify-cert [enable|disable]

```

```

    next
end
set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set http-multiplex [enable|disable]
set http-multiplex-ttl {integer}
set http-multiplex-max-request {integer}
set http-multiplex-max-concurrent-request {integer}
set http-ip-header [enable|disable]
set http-ip-header-name {string}
set outlook-web-access [disable|enable]
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
set ssl-mode [half|full]
set ssl-certificate <name1>, <name2>, ...
set ssl-dh-bits [768|1024|...]
set ssl-algorithm [high|medium|...]
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-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-pfs [require|deny|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-accept-ffdhe-groups [enable|disable]
set ssl-send-empty-frags [enable|disable]
set ssl-client-fallback [disable|enable]
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-type [disable|time|...]
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-max {integer}
set ssl-client-rekey-count {integer}
set ssl-server-renegotiation [enable|disable]
set ssl-server-session-state-type [disable|time|...]

```

```

set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-max {integer}
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-hpkp [disable|enable|...]
set ssl-hpkp-primary {string}
set ssl-hpkp-backup {string}
set ssl-hpkp-age {integer}
set ssl-hpkp-report-uri {var-string}
set ssl-hpkp-include-subdomains [disable|enable]
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set max-embryonic-connections {integer}
set one-click-gslb-server [disable|enable]
set gslb-hostname {string}
set gslb-domain-name {string}
config gslb-public-ips
    Description: Publicly accessible IP addresses for the FortiGSLB service.
    edit <index>
        set ip {ipv4-address-any}
    next
end
next
end

```

config firewall vip

Parameter	Description	Type	Size	Default
name	Virtual IP name.	string	Maximum length: 79	
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
comment	Comment.	var-string	Maximum length: 255	
type	Configure between a static NAT and access proxy VIP.	option	-	static-nat

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static-nat</i></td><td>Static NAT.</td></tr><tr><td><i>server-load-balance</i></td><td>Server load balance.</td></tr><tr><td><i>access-proxy</i></td><td>Access proxy.</td></tr></table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.	<i>access-proxy</i>	Access proxy.															
	Option	Description																						
	<i>static-nat</i>	Static NAT.																						
	<i>server-load-balance</i>	Server load balance.																						
<i>access-proxy</i>	Access proxy.																							
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.																							
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.																							
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																					

Parameter	Description	Type	Size	Default						
h2-support	Enable/disable 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	Enable/disable 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.									
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							
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35							
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.									
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.									

Parameter	Description	Type	Size	Default										
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.													
status	Enable/disable VIP.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the VIP.</td></tr><tr><td><i>enable</i></td><td>Enable the VIP.</td></tr></table>	Option	Description	<i>disable</i>	Disable the VIP.	<i>enable</i>	Enable the VIP.							
Option	Description													
<i>disable</i>	Disable the VIP.													
<i>enable</i>	Enable the VIP.													
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><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.													
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified											
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified											

Parameter	Description	Type	Size	Default								
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: 5 Maximum value: 8640000	0								
empty-cert-action	Action for an empty client certificate.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>block</i></td><td>Block the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>accept-unmanageable</i></td><td>Accept the SSL handshake only if the end-point is unmanageable.</td></tr></table>	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.			
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.											
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><i>disable</i></td><td>Disable detecting unknown devices by HTTP user-agent if no client certificate is provided.</td></tr><tr><td><i>enable</i></td><td>Enable detecting unknown devices by HTTP user-agent if no client certificate is provided.</td></tr></table>	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.					
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.											
client-cert	Enable/disable requesting client certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable client certificate request.</td></tr><tr><td><i>enable</i></td><td>Enable client certificate request.</td></tr></table>	Option	Description	<i>disable</i>	Disable client certificate request.	<i>enable</i>	Enable client certificate request.					
Option	Description											
<i>disable</i>	Disable client certificate request.											
<i>enable</i>	Enable client certificate request.											
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><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	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.					
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.											

Parameter	Description	Type	Size	Default						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
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-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-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.									
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.									
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.									

Parameter	Description	Type	Size	Default						
http-multiplex-ttl	Time-to-live for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15						
http-multiplex-max-request	Maximum number of requests that a multiplex server can handle before disconnecting sessions (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0						
http-multiplex-max-concurrent-request	Maximum number of concurrent requests that a multiplex server can handle (default = unlimited).	integer	Minimum value: 0 Maximum value: 2147483647	0						
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-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							
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>disable</td><td>Disable Outlook Web Access support.</td></tr><tr><td>enable</td><td>Enable Outlook Web Access support.</td></tr></table>				Option	Description	disable	Disable Outlook Web Access support.	enable	Enable Outlook Web Access support.
Option	Description									
disable	Disable Outlook Web Access support.									
enable	Enable Outlook Web Access support.									
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add HTTP header indicating SSL offload for WebLogic server.</td></tr><tr><td><i>enable</i></td><td>Add HTTP header indicating SSL offload for WebLogic server.</td></tr></table>	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.											
	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														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add HTTP header indicating SSL offload for WebSphere server.</td></tr><tr><td><i>enable</i></td><td>Add HTTP header indicating SSL offload for WebSphere server.</td></tr></table>	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.											
	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.																	
ssl-mode	Apply SSL offloading between the client and the FortiProxy (half) or from the client to the FortiProxy and from the FortiProxy to the server (full).	option	-	half														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>half</i></td><td>Client to FortiProxy SSL.</td></tr><tr><td><i>full</i></td><td>Client to FortiProxy and FortiProxy to Server SSL.</td></tr></table>	Option	Description	<i>half</i>	Client to FortiProxy SSL.	<i>full</i>	Client to FortiProxy and FortiProxy to Server SSL.											
	Option	Description																
	<i>half</i>	Client to FortiProxy SSL.																
<i>full</i>	Client to FortiProxy and FortiProxy to Server SSL.																	
ssl-certificate <name>	Name of the certificate to use for SSL handshake. Certificate list.	string	Maximum length: 79															
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-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-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><tr><td>custom</td><td>Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td>client</td><td>Use the same encryption algorithms for both client and server sessions.</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 ssl-server-cipher-suites to select the cipher suites that are allowed.	client	Use the same encryption algorithms for both client and server sessions.			
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 ssl-server-cipher-suites to select the cipher suites that are allowed.															
client	Use the same encryption algorithms for both client and server sessions.															
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.															

Parameter	Description	Type	Size	Default
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	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.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	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-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client
	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-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client

Parameter	Description	Type	Size	Default														
	<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-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-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-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-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-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiProxy.	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-client-session-state-timeout	Number of minutes to keep client to FortiProxy SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30										
ssl-client-session-state-max	Maximum number of client to FortiProxy SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000										
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576	0										
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-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiProxy.	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-server-session-state-timeout	Number of minutes to keep FortiProxy to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60										
ssl-server-session-state-max	Maximum number of FortiProxy to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100										
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-hpkp	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><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><tr><td><i>report-only</i></td><td>Add a HPKP Report-Only header to each 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.	<i>report-only</i>	Add a HPKP Report-Only header to each 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.										
<i>report-only</i>	Add a HPKP Report-Only header to each HTTP response.											
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79									
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79									
ssl-hpkp-age	Number of seconds the client should honor the HPKP setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000								
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255									
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-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								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	HSTS header does not apply to subdomains.		
	<i>enable</i>	HSTS header applies to subdomains.		
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000
one-click-gslb-server	Enable/disable one click GSLB server integration with FortiGSLB.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable integration with FortiGSLB.		
	<i>enable</i>	Enable integration with FortiGSLB.		
gslb-hostname	Hostname to use within the configured FortiGSLB domain.	string	Maximum length: 35	
gslb-domain-name	Domain to use when integrating with FortiGSLB.	string	Maximum length: 255	

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3

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						
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.									

config realservers

Parameter	Description	Type	Size	Default						
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
address	Dynamic address of the real server.	string	Maximum length: 79							
ip	IP address of the real server.	user	Not Specified							

Parameter	Description	Type	Size	Default
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
	Option	Description		
	active	Server status active.		
	standby	Server status standby.		
	disable	Server status disable.		
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
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
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	
	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
	Option	Description		
	ping	Use PING to test the link with the server.		
	http	Use HTTP-GET to test the link with the server.		
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
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.									
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						
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified							
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.									

config ssl-cipher-suites

Parameter	Description	Type	Size	Default						
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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></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.
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.									

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></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.			
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.																							

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></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-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.											
Option	Description															
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.															
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 ssl-server-cipher-suites

Parameter	Description	Type	Size	Default								
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0								
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></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.			
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.											

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></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-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-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
	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.			

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

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></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><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></table>	Option	Description	<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.	<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.			
Option	Description																									
<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.																									
<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.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	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.		
	TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	TLS-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	TLS-RSA-WITH-RC4-128-MD5	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		
	TLS-RSA-WITH-RC4-128-SHA	Cipher suite TLS-RSA-WITH-RC4-128-SHA.		
	TLS-DHE-RSA-WITH-DES-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.		
	TLS-DHE-DSS-WITH-DES-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.		
TLS-RSA-WITH-DES-CBC-SHA	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			

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
<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 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 firewall vipgrp

Configure IPv4 virtual IP groups.

```

config firewall vipgrp
  Description: Configure IPv4 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set interface {string}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
  next
end

```

config firewall vipgrp

Parameter	Description	Type	Size	Default
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
interface	Interface.	string	Maximum length: 35	
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). VIP name.	string	Maximum length: 79	

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 uuid {uuid}
    set wildcard-fqdn {string}
    set color {integer}
    set comment {var-string}
  next
end
```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 79	

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
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-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 uuid {uuid}
        set member <name1>, <name2>, ...
        set color {integer}
        set comment {var-string}
    next
end
```

config firewall wildcard-fqdn group

Parameter	Description	Type	Size	Default
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
member <name>	Address group members. Address name.	string	Maximum length: 79	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0

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

ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 513](#)

config ftp-proxy explicit

Configure explicit FTP proxy settings.

```
config ftp-proxy explicit
  Description: Configure explicit FTP proxy settings.
  set status [enable|disable]
  set incoming-port {user}
  set incoming-ip {ipv4-address-any}
  set outgoing-ip {ipv4-address-any}
  set sec-default-action [accept|deny]
  set server-data-mode [client|passive]
  set active-src-port [default|server]
  set ipv6-status [enable|disable]
  set incoming-ip6 {ipv6-address}
  set ssl [enable|disable]
  set ssl-cert <name1>, <name2>, ...
  set ssl-dh-bits [768|1024|...]
  set ssl-algorithm [high|medium|...]
end
```

config ftp-proxy explicit

Parameter	Description	Type	Size	Default
status	Enable/disable the explicit FTP proxy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the explicit FTP proxy.		
	<i>disable</i>	Disable the explicit FTP proxy.		
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified	
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

Parameter	Description	Type	Size	Default						
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>accept</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>deny</td><td>Deny requests unless there is a matching explicit FTP proxy policy.</td></tr></table>	Option	Description	accept	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not	deny	Deny requests unless there is a matching explicit FTP proxy policy.			
Option	Description									
accept	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not									
deny	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>client</td><td>Use the same transmission mode for client and server data sessions.</td></tr><tr><td>passive</td><td>Use passive mode on server data session.</td></tr></table>	Option	Description	client	Use the same transmission mode for client and server data sessions.	passive	Use passive mode on server data session.			
Option	Description									
client	Use the same transmission mode for client and server data sessions.									
passive	Use passive mode on server data session.									
active-src-port	Determine port for data session to connect FTP client in active mode.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Use the incoming port - 1 to connect client data session in active mode.</td></tr><tr><td>server</td><td>Use the same port as FTP server source port to connect client data session in active mode.</td></tr></table>	Option	Description	default	Use the incoming port - 1 to connect client data session in active mode.	server	Use the same port as FTP server source port to connect client data session in active mode.			
Option	Description									
default	Use the incoming port - 1 to connect client data session in active mode.									
server	Use the same port as FTP server source port to connect client data session in active mode.									
ipv6-status	Enable/disable allowing an IPv6 ftp 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>enable</td><td>Enable allowing an IPv6 ftp proxy destination.</td></tr><tr><td>disable</td><td>Disable allowing an IPv6 ftp proxy destination.</td></tr></table>	Option	Description	enable	Enable allowing an IPv6 ftp proxy destination.	disable	Disable allowing an IPv6 ftp proxy destination.			
Option	Description									
enable	Enable allowing an IPv6 ftp proxy destination.									
disable	Disable allowing an IPv6 ftp proxy destination.									
incoming-ip6	Restrict the explicit ftp proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::						
ssl	Enable/disable the explicit FTPS 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 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-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.													
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.													

hardware

This section includes syntax for the following commands:

- [config hardware cpu on page 516](#)
- [config hardware memory on page 516](#)
- [config hardware nic on page 516](#)
- [config hardware status on page 517](#)

config hardware cpu

Display detailed information for all installed CPU(s).

```
config hardware cpu
    Description: Display detailed information for all installed CPU(s).
end
```

config hardware memory

Display system memory information.

```
config hardware memory
    Description: Display system memory information.
end
```

config hardware nic

Display NIC information.

```
config hardware nic
    Description: Display NIC information.
    set <nic> {string}
end
```

config hardware nic

Parameter	Description	Type	Size	Default
<nic>	NIC name.	string	Maximum length: -	

config hardware status

Hardware status.

```
config hardware status
    Description: Hardware status.
end
```

icap

This section includes syntax for the following commands:

- [config icap local-server on page 518](#)
- [config icap profile on page 521](#)
- [config icap remote-server-group on page 531](#)
- [config icap remote-server on page 530](#)

config icap local-server

Configure ICAP local server.

```
config icap local-server
  Description: Configure ICAP local server.
  edit <icap-server-id>
    set status [disable|enable]
    set secure-connection [disable|enable]
    set status-ipv6 [disable|enable]
    set icap-incoming-port {integer}
    set icap-incoming-ssl-port {integer}
    set interface {string}
    set incoming-ip {ipv4-address-any}
    set incoming-ipv6 {ipv6-address}
    set ssl-cert <name1>, <name2>, ...
    set strict-scheme-check [disable|enable]
    set message-preview [disable|enable]
    set srcaddr {string}
    set timeout {integer}
  config icap-service
    Description: Set up services for local ICAP server.
    edit <service-id>
      set name {string}
      set dlp-profile {string}
      set av-profile {string}
      set webfilter-profile {string}
      set image-analyzer-profile {string}
      set profile-protocol-options {string}
      set extension-headers {option1}, {option2}, ...
    next
  end
next
end
```

config icap local-server

Parameter	Description	Type	Size	Default						
icap-server-id	ICAP local server id.	integer	Minimum value: 0 Maximum value: 65535	0						
status	Enable/disable status for icap server network profile.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the status for ipv4 in network-profile.</td></tr><tr><td>enable</td><td>Enable the status for ipv4 in network-profile.</td></tr></table>	Option	Description	disable	Disable the status for ipv4 in network-profile.	enable	Enable the status for ipv4 in network-profile.			
Option	Description									
disable	Disable the status for ipv4 in network-profile.									
enable	Enable the status for ipv4 in network-profile.									
secure-connection	Enable/disable status for secured icap server network profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the status for ipv4 ssl in network-profile.</td></tr><tr><td>enable</td><td>Enable the status for ipv4 ssl in network-profile.</td></tr></table>	Option	Description	disable	Disable the status for ipv4 ssl in network-profile.	enable	Enable the status for ipv4 ssl in network-profile.			
Option	Description									
disable	Disable the status for ipv4 ssl in network-profile.									
enable	Enable the status for ipv4 ssl in network-profile.									
status-ipv6	Enable/disable status for icap server service ipv6.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the status for ipv6 in network-profile.</td></tr><tr><td>enable</td><td>Enable the status for ipv6 in network-profile.</td></tr></table>	Option	Description	disable	Disable the status for ipv6 in network-profile.	enable	Enable the status for ipv6 in network-profile.			
Option	Description									
disable	Disable the status for ipv6 in network-profile.									
enable	Enable the status for ipv6 in network-profile.									
icap-incoming-port	Accept incoming ICAP requests on a port (0 - 65535, default = 1344).	integer	Minimum value: 1 Maximum value: 65535	1344						
icap-incoming-ssl-port	Accept incoming secured ICAP requests on a port (0 - 65535, default = 11344).	integer	Minimum value: 1 Maximum value: 65535	11344						
interface	Interface name	string	Maximum length: 15							

Parameter	Description	Type	Size	Default						
incoming-ip	Restrict the ICAP server 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-ipv6	Restrict the ICAP server to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::						
ssl-cert <name>	SSL certificate for SSL interception. Certificate list.	string	Maximum length: 79							
strict-scheme-check	Enable/disable strict check of scheme.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable strict check of scheme.</td></tr><tr><td><i>enable</i></td><td>Enable strict check of scheme.</td></tr></table>				Option	Description	<i>disable</i>	Disable strict check of scheme.	<i>enable</i>	Enable strict check of scheme.
Option	Description									
<i>disable</i>	Disable strict check of scheme.									
<i>enable</i>	Enable strict check of scheme.									
message-preview	Enable/disable message preview support. Max preview data length is 4096 bytes.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable message preview support.</td></tr><tr><td><i>enable</i></td><td>Enable message preview support.</td></tr></table>				Option	Description	<i>disable</i>	Disable message preview support.	<i>enable</i>	Enable message preview support.
Option	Description									
<i>disable</i>	Disable message preview support.									
<i>enable</i>	Enable message preview support.									
srcaddr	Source address name.	string	Maximum length: 79							
timeout	ICAP server idle timeout in seconds.	integer	Minimum value: 30 Maximum value: 3600	300						

config icap-service

Parameter	Description	Type	Size	Default
service-id	ID of the ICAP server service.	integer	Minimum value: 0 Maximum value: 65535	0
name	Name of ICAP service profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 35	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
image-analyzer-profile	Name of an existing Image analyzer profile.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
extension-headers	Configure the extension headers of icap server response.	option	-	
	Option	Description		
	X-Virus-id	Enable X-Virus-ID ICAP extension header.		
	X-Infection-Found	Enable X-Infection-Found ICAP extension header.		
	X-Violation-Found	Enable X-Violation-Found ICAP extension header.		

config icap profile

Configure ICAP profiles.

```

config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    set replacemsg-group {string}
    set comment {var-string}
    set request [disable|enable]
    set response [disable|enable]
    set file-transfer {option1}, {option2}, ...
    set streaming-content-bypass [disable|enable]
    set ocr_only [disable|enable]
    set 204-size-limit {integer}
    set 204-response [disable|enable]
    set preview [disable|enable]
    set preview-data-length {integer}
    set request-server {string}
    set response-server {string}

```

```

set file-transfer-server {string}
set request-failure [error|bypass]
set response-failure [error|bypass]
set file-transfer-failure [error|bypass]
set request-path {string}
set response-path {string}
set file-transfer-path {string}
set methods {option1}, {option2}, ...
set response-req-hdr [disable|enable]
set respmod-default-action [forward|bypass]
set icap-block-log [disable|enable]
set chunk-encap [disable|enable]
set extension-feature {option1}, {option2}, ...
set scan-progress-interval {integer}
set timeout {integer}
set scan-size-limit {integer}
set scan-oversize-log [disable|enable]
config icap-headers
    Description: Configure ICAP forwarded request headers.
    edit <id>
        set name {string}
        set source [content|http-header|...]
        set content {string}
        set http-header {string}
        set session-info-type [client-ip|user|...]
        set base64-encoding [disable|enable]
    next
end
config respmod-forward-rules
    Description: ICAP response mode forward rules.
    edit <name>
        set host {string}
        config header-group
            Description: HTTP header group.
            edit <id>
                set header-name {string}
                set header {string}
                set case-sensitivity [disable|enable]
            next
        end
        set action [forward|bypass]
        set http-resp-status-code <code1>, <code2>, ...
    next
end
next
end

```

config icap profile

Parameter	Description	Type	Size	Default						
replacemsg-group	Replacement message group.	string	Maximum length: 35							
name	ICAP profile name.	string	Maximum length: 35							
comment	Comment.	var-string	Maximum length: 255							
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><i>disable</i></td><td>Disable HTTP request passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP request passing to ICAP server.</td></tr></table>	Option	Description	<i>disable</i>	Disable HTTP request passing to ICAP server.	<i>enable</i>	Enable HTTP request passing to ICAP server.			
Option	Description									
<i>disable</i>	Disable HTTP request passing to ICAP server.									
<i>enable</i>	Enable HTTP request passing to ICAP server.									
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><i>disable</i></td><td>Disable HTTP response passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP response passing to ICAP server.</td></tr></table>	Option	Description	<i>disable</i>	Disable HTTP response passing to ICAP server.	<i>enable</i>	Enable HTTP response passing to ICAP server.			
Option	Description									
<i>disable</i>	Disable HTTP response passing to ICAP server.									
<i>enable</i>	Enable HTTP response passing to ICAP server.									
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><i>ssh</i></td><td>Forward file transfer with SSH protocol to ICAP server for further processing.</td></tr><tr><td><i>ftp</i></td><td>Forward file transfer with FTP protocol to ICAP server for further processing.</td></tr></table>	Option	Description	<i>ssh</i>	Forward file transfer with SSH protocol to ICAP server for further processing.	<i>ftp</i>	Forward file transfer with FTP protocol to ICAP server for further processing.			
Option	Description									
<i>ssh</i>	Forward file transfer with SSH protocol to ICAP server for further processing.									
<i>ftp</i>	Forward file transfer with FTP protocol to ICAP server for further processing.									
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.									

Parameter	Description	Type	Size	Default
ocr_only	Enable/disable only passing OCR scan request to ICAP server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable only passing OCR scan request to ICAP server.		
	<i>enable</i>	Enable only passing OCR scan request to ICAP server.		
204-size-limit	Allow 204 size limit to be saved by ICAP client. (default = 1 MB)	integer	Minimum value: 1 Maximum value: 10	1
204-response	Enable/disable allowance of 204 response from ICAP server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable allowance of 204 response from ICAP server.		
	<i>enable</i>	Enable allowance of 204 response from 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.		
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096	0
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 63	
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 63	
file-transfer-server	ICAP server to use for a file transfer.	string	Maximum length: 63	
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error.		
	<i>bypass</i>	Bypass.		
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-	error
	Option	Description		
	<i>error</i>	Error.		
	<i>bypass</i>	Bypass.		
file-transfer-failure	Action to take if the ICAP server cannot be contacted when processing a file transfer.	option	-	error
	Option	Description		
	<i>error</i>	Error.		
	<i>bypass</i>	Bypass.		
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127	
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127	
file-transfer-path	Path component of the ICAP URI that identifies the file transfer processing service.	string	Maximum length: 127	
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
	Option	Description		
	<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>get</i></td><td>Forward HTTP request or response with GET method to ICAP server for further processing.</td></tr><tr><td><i>head</i></td><td>Forward HTTP request or response with HEAD method to ICAP server for further processing.</td></tr><tr><td><i>options</i></td><td>Forward HTTP request or response with OPTIONS method to ICAP server for further processing.</td></tr><tr><td><i>post</i></td><td>Forward HTTP request or response with POST method to ICAP server for further processing.</td></tr><tr><td><i>put</i></td><td>Forward HTTP request or response with PUT method to ICAP server for further processing.</td></tr><tr><td><i>trace</i></td><td>Forward HTTP request or response with TRACE method to ICAP server for further processing.</td></tr><tr><td><i>connect</i></td><td>Forward HTTP request or response with CONNECT method to ICAP server for further processing.</td></tr><tr><td><i>other</i></td><td>Forward HTTP request or response with All other methods to ICAP server for further processing.</td></tr></table>	Option	Description	<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.			
	Option	Description																				
	<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.																					
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.																					
respmod-default-action	Default action to ICAP response modification (respmod) processing.	option	-	forward																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward response to ICAP server unless a rule specifies not to.</td></tr><tr><td><i>bypass</i></td><td>Don't forward request to ICAP server unless a rule specifies to forward the request.</td></tr></table>	Option	Description	<i>forward</i>	Forward response to ICAP server unless a rule specifies not to.	<i>bypass</i>	Don't forward request to ICAP server unless a rule specifies to forward the request.															
	Option	Description																				
	<i>forward</i>	Forward response to ICAP server unless a rule specifies not to.																				
<i>bypass</i>	Don't forward request to ICAP server unless a rule specifies to forward the request.																					
icap-block-log	Enable/disable UTM log when infection found (default = disable).	option	-	disable																		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable UTM log when infection found.		
	<i>enable</i>	Enable UTM log when infection found.		
chunk-encap	Enable/disable chunked encapsulation (default = disable).	option	-	disable
	Option Description			
	<i>disable</i>	Do not encapsulate chunked data.		
	<i>enable</i>	Encapsulate chunked data into a new chunk.		
extension-feature	Enable/disable ICAP extension features.	option	-	
	Option Description			
	<i>scan-progress</i>	Support X-Scan-Progress-Interval ICAP header.		
scan-progress-interval	Scan progress interval value.	integer	Minimum value: 5 Maximum value: 30	10
timeout	Time (in seconds) that ICAP client waits for the response from ICAP server.	integer	Minimum value: 30 Maximum value: 3600	30
scan-size-limit	ICAP server scan size limit for an single request. (0 - 4096 MB, default = 0 MB means unlimited)	integer	Minimum value: 0 Maximum value: 4096	0
scan-oversize-log	Enable/disable scan oversize log (default = enable).	option	-	enable
	Option Description			
	<i>disable</i>	Disable scan oversize log.		
	<i>enable</i>	Enable scan oversize log.		

config icap-headers

Parameter	Description	Type	Size	Default
id	HTTP forwarded header ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	HTTP forwarded header name.	string	Maximum length: 79	
source	HTTP append header source.	option	-	content
	Option	Description		
	content	Create ICAP header from content.		
	http-header	Create ICAP header from HTTP header.		
	session	Create ICAP header from session info.		
content	HTTP header content.	string	Maximum length: 255	
http-header	HTTP header-field name.	string	Maximum length: 79	
session-info-type	Session info type.	option	-	client-ip
	Option	Description		
	client-ip	Client ip address.		
	user	Authentication user name.		
	upn	Authentication user principal name.		
	domain	User domain name.		
	local-grp	Firewall group name.		
	remote-grp	Group name from authentication server.		
	proxy-name	Proxy realm name.		
	auth-user-uri	Authenticated user uri.		
	auth-group-uri	Authenticated group uri.		
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable use of base64 encoding of HTTP content.		
	<i>enable</i>	Enable use of base64 encoding of HTTP content.		

config respmod-forward-rules

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 63	
host	Address object for the host.	string	Maximum length: 79	
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.		
http-resp-status-code <code>	HTTP response status code. HTTP response status code.	integer	Minimum value: 100 Maximum value: 599	

config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Enable/disable case sensitivity when matching header.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Ignore case when matching header.		
	<i>enable</i>	Do not ignore case when matching header.		

config icap remote-server

Configure ICAP servers.

```

config icap remote-server
    Description: Configure ICAP servers.
    edit <name>
        set addr-type [ip4|ip6|...]
        set ip-address {ipv4-address-any}
        set ip6-address {ipv6-address}
        set fqdn {string}
        set secure [disable|enable]
        set port {integer}
        set max-connections {integer}
        set ssl-cert {string}
        set healthcheck [disable|enable]
        set healthcheck-service {string}
    next
end

```

config icap remote-server

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 63	
addr-type	Address type of the remote ICAP server: IPv4, IPv6 or FQDN.	option	-	ip4
	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 remote ICAP server.		
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::						
fqdn	ICAP remote server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255							
secure	Enable/disable secure connection to ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable connection to secure ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable connection to secure ICAP server.</td></tr></table>				Option	Description	<i>disable</i>	Disable connection to secure ICAP server.	<i>enable</i>	Enable connection to secure ICAP server.
Option	Description									
<i>disable</i>	Disable connection to secure ICAP server.									
<i>enable</i>	Enable connection to secure ICAP server.									
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344						
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						
ssl-cert	CA certificate name.	string	Maximum length: 79							
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><i>disable</i></td><td>Disable health checking.</td></tr><tr><td><i>enable</i></td><td>Enable health checking.</td></tr></table>				Option	Description	<i>disable</i>	Disable health checking.	<i>enable</i>	Enable health checking.
Option	Description									
<i>disable</i>	Disable health checking.									
<i>enable</i>	Enable health checking.									
healthcheck-service	ICAP Service name to use for health checks.	string	Maximum length: 127							

config icap remote-server-group

Configure an ICAP remote server group consisting of multiple forward servers. Supports failover and load balancing.

```
config icap remote-server-group
    Description: Configure an ICAP remote 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 remote 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 remote-server-group

Parameter	Description	Type	Size	Default								
name	Configure an ICAP remote server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63									
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.											

config server-list

Parameter	Description	Type	Size	Default
name	ICAP remote 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

image-analyzer

This section includes syntax for the following commands:

- [config image-analyzer profile on page 533](#)

config image-analyzer profile

Configure image analyzer profiles

```
config image-analyzer profile
  Description: Configure image analyzer profiles
  edit <name>
    set comment {var-string}
    set alcohol-block-strictness-level {integer}
    set alcohol-status [allow|deny|...]
    set drugs-block-strictness-level {integer}
    set drugs-status [allow|deny|...]
    set extremism-block-strictness-level {integer}
    set extremism-status [allow|deny|...]
    set gambling-block-strictness-level {integer}
    set gambling-status [allow|deny|...]
    set gore-block-strictness-level {integer}
    set gore-status [allow|deny|...]
    set porn-block-strictness-level {integer}
    set porn-status [allow|deny|...]
    set swim_underwear-block-strictness-level {integer}
    set swim_underwear-status [allow|deny|...]
    set weapons-block-strictness-level {integer}
    set weapons-status [allow|deny|...]
    set image-skip-size {integer}
    set image-skip-width {integer}
    set image-skip-height {integer}
    set log-option [all|violation]
    set source-url [enable|disable]
    set blocked-img-cache [enable|disable]
    set rating-err-action [block|pass]
    set replace-image {string}
    set optical-character-recognition [enable|disable]
    set ocr-activation-threshold {integer}
  next
end
```

config image-analyzer profile

Parameter	Description	Type	Size	Default								
name	Profile name.	string	Maximum length: 35									
comment	Comment.	var-string	Maximum length: 255									
alcohol-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30								
alcohol-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
drugs-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30								
drugs-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
extremism-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30								
extremism-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											

Parameter	Description	Type	Size	Default
gambling-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30
gambling-status	Allow/deny/monitor the category image.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
gore-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30
gore-status	Allow/deny/monitor the category image.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
porn-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30
porn-status	Allow/deny/monitor the category image.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
swim_underwear-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30

Parameter	Description	Type	Size	Default
swim_underwear-status	Allow/deny/monitor the category image.	option	-	deny
	Option Description			
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
weapons-block-strictness-level	Higher value means an image is more likely to be blocked(0 - 100, 0 = allow all images, 100 = block all images).	integer	Minimum value: 0 Maximum value: 100	30
weapons-status	Allow/deny/monitor the category image.	option	-	deny
	Option Description			
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
image-skip-size	Image skip rating size(0-2048k).	integer	Minimum value: 0 Maximum value: 2048	1
image-skip-width	Image skip rating width(min. 5 pixel).	integer	Minimum value: 5 Maximum value: 2147483647	30
image-skip-height	Image skip rating height(min. 5 pixel).	integer	Minimum value: 5 Maximum value: 2147483647	30
log-option	Log option for the inspected image result.	option	-	violation
	Option Description			
	<i>all</i>	Log all image result.		
	<i>violation</i>	Log only violation image result.		

Parameter	Description	Type	Size	Default						
source-url	Enable/disable source url in the image search result.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source url in image search.</td></tr><tr><td><i>disable</i></td><td>Disable source url in image search.</td></tr></table>	Option	Description	<i>enable</i>	Enable source url in image search.	<i>disable</i>	Disable source url in image search.			
Option	Description									
<i>enable</i>	Enable source url in image search.									
<i>disable</i>	Disable source url in image search.									
blocked-img-cache	Enable/disable saving blocked images in ram disk.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable caching.</td></tr><tr><td><i>disable</i></td><td>Disable caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable caching.	<i>disable</i>	Disable caching.			
Option	Description									
<i>enable</i>	Enable caching.									
<i>disable</i>	Disable caching.									
rating-err-action	Actions when image rating error.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block.</td></tr><tr><td><i>pass</i></td><td>Pass.</td></tr></table>	Option	Description	<i>block</i>	Block.	<i>pass</i>	Pass.			
Option	Description									
<i>block</i>	Block.									
<i>pass</i>	Pass.									
replace-image	Specify replacement image.	string	Maximum length: 35							
optical-character-recognition	Enable/disable optical character recognition.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable optical character recognition.</td></tr><tr><td><i>disable</i></td><td>Disable optical character recognition.</td></tr></table>	Option	Description	<i>enable</i>	Enable optical character recognition.	<i>disable</i>	Disable optical character recognition.			
Option	Description									
<i>enable</i>	Enable optical character recognition.									
<i>disable</i>	Disable optical character recognition.									
ocr-activation-threshold	Threshold to activate optical character recognition(0 - 100, 0 = bypass all images without DLP, 100 = process all images with DLP).	integer	Minimum value: 0 Maximum value: 100	30						

ips

This section includes syntax for the following commands:

- [config ips custom on page 538](#)
- [config ips decoder on page 540](#)
- [config ips global on page 540](#)
- [config ips rule-settings on page 546](#)
- [config ips rule on page 544](#)
- [config ips sensor on page 546](#)
- [config ips session on page 552](#)
- [config ips settings on page 553](#)
- [config ips view-map on page 554](#)

config ips custom

Configure IPS custom signature.

```
config ips custom
  Description: Configure IPS custom signature.
  edit <tag>
    set signature {var-string}
    set rule-id {integer}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set protocol {user}
    set status [disable|enable]
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set comment {string}
  next
end
```

config ips custom

Parameter	Description	Type	Size	Default
tag	Signature tag.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095							
rule-id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified							
location	Protect client or server traffic.	user	Not Specified							
os	Operating system(s) that the signature protects. Blank for all operating systems.	user	Not Specified							
application	Applications to be protected. Blank for all applications.	user	Not Specified							
protocol	Protocol(s) that the signature scans. Blank for all protocols.	user	Not Specified							
status	Enable/disable this signature.	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.									
log	Enable/disable logging.	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.	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.									
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.		
comment	Comment.	string	Maximum length: 63	

config ips decoder

Configure IPS decoder.

```
config ips decoder
  Description: Configure IPS decoder.
  edit <name>
    config parameter
      Description: IPS group parameters.
      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 fail-open [enable|disable]
    set database [regular|extended]
    set traffic-submit [enable|disable]
    set anomaly-mode [periodical|continuous]
    set session-limit-mode [accurate|heuristic]
    set socket-size {integer}
    set engine-count {integer}
    set sync-session-ttl [enable|disable]
    set deep-app-insp-timeout {integer}
    set deep-app-insp-db-limit {integer}
    set exclude-signatures [none|ot]
    set packet-log-queue-depth {integer}
    set av-mem-limit {integer}
    config tls-active-probe
        Description: TLS active probe configuration.
        set interface-select-method [auto|sdwan|...]
        set interface {string}
        set vdom {string}
        set source-ip {ipv4-address}
        set source-ip6 {ipv6-address}
    end
end

```

config ips global

Parameter	Description	Type	Size	Default						
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						
	<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.									
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><i>regular</i></td><td>IPS regular database package.</td></tr><tr><td><i>extended</i></td><td>IPS extended database package.</td></tr></table>	Option	Description	<i>regular</i>	IPS regular database package.	<i>extended</i>	IPS extended database package.			
Option	Description									
<i>regular</i>	IPS regular database package.									
<i>extended</i>	IPS extended database package.									

Parameter	Description	Type	Size	Default						
traffic-submit	Enable/disable submitting attack data found by this FortiProxy to FortiGuard.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable traffic submit.</td></tr><tr><td><i>disable</i></td><td>Disable traffic submit.</td></tr></table>	Option	Description	<i>enable</i>	Enable traffic submit.	<i>disable</i>	Disable traffic submit.			
Option	Description									
<i>enable</i>	Enable traffic submit.									
<i>disable</i>	Disable traffic submit.									
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.									
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accurate</i></td><td>Accurately count concurrent sessions, demands more resources.</td></tr><tr><td><i>heuristic</i></td><td>Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.</td></tr></table>	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.			
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: 0 Maximum value: 128	64						
engine-count	Number of IPS engines running. If set to the default value of 0, FortiProxy sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0						
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of kernel session TTL for IPS sessions.</td></tr><tr><td><i>disable</i></td><td>Disable use of kernel session TTL for IPS sessions.</td></tr></table>	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.			
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.									

Parameter	Description	Type	Size	Default
deep-app-insp-timeout	Timeout for Deep application inspection (1 - 2147483647 sec., 0 = use recommended setting).	integer	Minimum value: 0 Maximum value: 2147483647	0
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 Maximum value: 2147483647	0
exclude-signatures	Excluded signatures.	option	-	ot
	Option		Description	
	<i>none</i>		No signatures excluded.	
	<i>ot</i>		Exclude ot signatures.	
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128
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: 10 Maximum value: 50	0

config tls-active-probe

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.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31	
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	::

config ips rule

Configure IPS rules.

```

config ips rule
    Description: Configure IPS rules.
    edit <name>
        set log [disable|enable]
        set log-packet [disable|enable]
        set action [pass|block]
        set group {string}
        set severity {user}
        set location {user}
        set os {user}
        set application {user}
        set service {user}
        set rule-id {integer}
        set rev {integer}
        set date {integer}
        config metadata
            Description: Meta data.
            edit <id>
                set metaid {integer}
                set valueid {integer}
            next
        end
    next
end

```

config ips rule

Parameter	Description	Type	Size	Default
name	Rule name.	string	Maximum length: 63	
log	Enable/disable logging.	option	-	enable

Parameter	Description	Type	Size	Default
	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.		
action	Action.	option	-	pass
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
group	Group.	string	Maximum length: 63	
severity	Severity.	user	Not Specified	
location	Vulnerable location.	user	Not Specified	
os	Vulnerable operation systems.	user	Not Specified	
application	Vulnerable applications.	user	Not Specified	
service	Vulnerable service.	user	Not Specified	
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ips rule-settings

Configure IPS rule setting.

```
config ips rule-settings
    Description: Configure IPS rule setting.
    edit <id>
    next
end
```

config ips rule-settings

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

config ips sensor

Configure IPS sensor.

```

config ips sensor
    Description: Configure IPS sensor.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set block-malicious-url [disable|enable]
        set scan-botnet-connections [disable|block|...]
        set extended-log [enable|disable]
    config entries
        Description: IPS sensor filter.
        edit <id>
            set rule <id1>, <id2>, ...
            set location {user}
            set severity {user}
            set protocol {user}
            set os {user}
            set application {user}
            set default-action [all|pass|...]
            set default-status [all|enable|...]
            set cve <cve-entry1>, <cve-entry2>, ...
            set vuln-type <id1>, <id2>, ...
            set last-modified {user}
            set status [disable|enable|...]
            set log [disable|enable]
            set log-packet [disable|enable]
            set log-attack-context [disable|enable]
            set action [pass|block|...]
            set rate-count {integer}
            set rate-duration {integer}
            set rate-mode [periodical|continuous]
            set rate-track [none|src-ip|...]
        config exempt-ip
            Description: Traffic from selected source or destination IP addresses is
exempt from this signature.
            edit <id>
                set src-ip {ipv4-classnet}
                set dst-ip {ipv4-classnet}
            next
        end
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
    next
end
next
end

```

config ips sensor

Parameter	Description	Type	Size	Default								
name	Sensor name.	string	Maximum length: 35									
comment	Comment.	var-string	Maximum length: 255									
replacemsg-group	Replacement message group.	string	Maximum length: 35									
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable malicious URL blocking.</td></tr><tr><td><i>enable</i></td><td>Enable malicious URL blocking.</td></tr></table>				Option	Description	<i>disable</i>	Disable malicious URL blocking.	<i>enable</i>	Enable malicious URL blocking.		
Option	Description											
<i>disable</i>	Disable malicious URL blocking.											
<i>enable</i>	Enable malicious URL blocking.											
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not scan connections to botnet servers.</td></tr><tr><td><i>block</i></td><td>Block connections to botnet servers.</td></tr><tr><td><i>monitor</i></td><td>Log connections to botnet servers.</td></tr></table>				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.
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.											
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.											

config entries

Parameter	Description	Type	Size	Default
id	Rule ID in IPS database (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295									
location	Protect client or server traffic.	user	Not Specified	all								
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all								
protocol	Protocols to be examined. Use all for every protocol and other for unlisted protocols.	user	Not Specified	all								
os	Operating systems to be protected. Use all for every operating system and other for unlisted operating systems.	user	Not Specified	all								
application	Operating systems to be protected. Use all for every application and other for unlisted application.	user	Not Specified	all								
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.											
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor. CVE IDs or CVE wildcards.	string	Maximum length: 19									

Parameter	Description	Type	Size	Default								
vuln-type <id>	List of signature vulnerability types to filter by. Vulnerability type ID.	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									
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>disable</td><td>Disable status of selected rules.</td></tr><tr><td>enable</td><td>Enable status of selected rules.</td></tr><tr><td>default</td><td>Default.</td></tr></table>	Option	Description	disable	Disable status of selected rules.	enable	Enable status of selected rules.	default	Default.			
Option	Description											
disable	Disable status of selected rules.											
enable	Enable status of selected rules.											
default	Default.											
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-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>disable</td><td>Disable packet logging of selected rules.</td></tr><tr><td>enable</td><td>Enable packet logging of selected rules.</td></tr></table>	Option	Description	disable	Disable packet logging of selected rules.	enable	Enable packet logging of selected rules.					
Option	Description											
disable	Disable packet logging of selected rules.											
enable	Enable packet logging of selected rules.											
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of detailed attack context.</td></tr><tr><td>enable</td><td>Enable logging of detailed attack context.</td></tr></table>	Option	Description	disable	Disable logging of detailed attack context.	enable	Enable logging of detailed attack context.					
Option	Description											
disable	Disable logging of detailed attack context.											
enable	Enable logging of detailed attack context.											

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.		
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous
	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
	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.		
quarantine	Quarantine method.	option	-	none
	Option	Description		
	<i>none</i>	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 <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.									

config exempt-ip

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

config ips session

Session status.

```
config ips session
    Description: Session status.
end
```

config ips settings

Configure IPS VDOM parameter.

```
config ips settings
  Description: Configure IPS VDOM parameter.
  set packet-log-history {integer}
  set packet-log-post-attack {integer}
  set packet-log-memory {integer}
  set ips-packet-quota {integer}
  set proxy-inline-ips [disable|enable]
end
```

config ips settings

Parameter	Description	Type	Size	Default
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 Maximum value: 255	1
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
packet-log-memory	Maximum memory can be used by packet log (64 - 8192 kB).	integer	Minimum value: 64 Maximum value: 8192	256
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 Maximum value: 4294967295	0
proxy-inline-ips	Enable/disable firewall policy inline IPS support.	option	-	enable
		Option	Description	
		<i>disable</i>	Do not allow inline IPS in firewall policy.	
		<i>enable</i>	Allow inline IPS in firewall policy.	

config ips view-map

Configure IPS view-map.

```
config ips view-map
  Description: Configure IPS view-map.
  edit <id>
    set vdom-id {integer}
    set policy-id {integer}
    set id-policy-id {integer}
    set which {option}
  next
end
```

config ips view-map

Parameter	Description	Type	Size	Default
id	View ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
vdom-id	VDOM ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
policy-id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
id-policy-id	ID-based policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
which	Policy.	option	-	firewall
		Option	Description	
		<i>firewall</i>	Firewall policy.	

ipsec

This section includes syntax for the following commands:

- [config ipsec tunnel on page 555](#)

config ipsec tunnel

IPsec tunnel.

```
config ipsec tunnel
    Description: IPsec tunnel.
end
```

isolator

This section includes syntax for the following commands:

- [config isolator profile on page 556](#)
- [config isolator setting on page 557](#)

config isolator profile

Configure isolator profiles.

```
config isolator profile
  Description: Configure isolator profiles.
  edit <name>
    set comments {var-string}
    set disclaimer {string}
    config entries
      Description: Isolator profile entries.
      edit <id>
        set proxy-address {string}
        set action [isolate|freeze|...]
        set status [enable|disable]
      next
    end
  next
end
```

config isolator profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 255	
disclaimer	A customized replacement message page for installer.	string	Maximum length: 35	

config entries

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
proxy-address	Choose the proxy-address for this isolator profile entry.	string	Maximum length: 79	
action	Choose the action for this isolator entry.	option	-	isolate
	Option	Description		
	isolate	Open the website in an isolator instead of the client.		
	freeze	Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk.		
	block	Block the traffic to the website.		
	allow	Bypass the traffic to the website.		
status	Enable/disable this isolator entry.	option	-	enable
	Option	Description		
	enable	Enable this entry.		
	disable	Disable this entry.		

config isolator setting

Configure isolator setting.

```
config isolator setting
  Description: Configure isolator setting.
  set default-isolator-profile {string}
  set defective-session [use-default-profile|pass|...]
  set unmatched-session [use-default-profile|pass|...]
end
```

config isolator setting

Parameter	Description	Type	Size	Default
default-isolator-profile	Name of an existing isolator profile. This profile is used when no policy is matched.	string	Maximum length: 35	
defective-session	Choose the way to handle rating requests for sessions with missing information.	option	-	pass
	Option	Description		
	<i>use-default-profile</i>	Use default isolator profile to handle the session.		
	<i>pass</i>	Return bypass response to the rating request of the session.		
	<i>block</i>	Return block response to the rating request of the session.		
unmatched-session	Choose the way to handle rating requests for sessions that are unable to match any policy.	option	-	pass
	Option	Description		
	<i>use-default-profile</i>	Use default isolator profile to handle the session.		
	<i>pass</i>	Return bypass response to the rating request of the session.		
	<i>block</i>	Return block response to the rating request of the session.		

I2vpn

This section includes syntax for the following commands:

- [config l2vpn evpn instance on page 559](#)
- [config l2vpn evpn table on page 559](#)

config l2vpn evpn instance

List EVPN instances.

```
config l2vpn evpn instance
  Description: List EVPN instances.
  set <id> {string}
end
```

config l2vpn evpn instance

Parameter	Description	Type	Size	Default
<id>	EVPN ID.	string	Maximum length: -	

config l2vpn evpn table

List EVPN tables.

```
config l2vpn evpn table
  Description: List EVPN tables.
  set <ID> {string}
end
```

config l2vpn evpn table

Parameter	Description	Type	Size	Default
<ID>	EVPN ID ('-' for all).	string	Maximum length: -	

log

This section includes syntax for the following commands:

- [config log custom-field on page 561](#)
- [config log disk filter on page 562](#)
- [config log disk setting on page 565](#)
- [config log eventfilter on page 571](#)
- [config log fortianalyzer-cloud filter on page 624](#)
- [config log fortianalyzer-cloud override-filter on page 628](#)
- [config log fortianalyzer-cloud override-setting on page 631](#)
- [config log fortianalyzer-cloud setting on page 632](#)
- [config log fortianalyzer2 filter on page 591](#)
- [config log fortianalyzer2 override-filter on page 595](#)
- [config log fortianalyzer2 override-setting on page 599](#)
- [config log fortianalyzer2 setting on page 603](#)
- [config log fortianalyzer3 filter on page 608](#)
- [config log fortianalyzer3 override-filter on page 611](#)
- [config log fortianalyzer3 override-setting on page 615](#)
- [config log fortianalyzer3 setting on page 620](#)
- [config log fortianalyzer filter on page 575](#)
- [config log fortianalyzer override-filter on page 579](#)
- [config log fortianalyzer override-setting on page 582](#)
- [config log fortianalyzer setting on page 587](#)
- [config log fortiguard filter on page 636](#)
- [config log fortiguard override-filter on page 639](#)
- [config log fortiguard override-setting on page 643](#)
- [config log fortiguard setting on page 644](#)
- [config log gui-display on page 647](#)
- [config log memory filter on page 648](#)
- [config log memory global-setting on page 652](#)
- [config log memory setting on page 652](#)
- [config log null-device filter on page 653](#)
- [config log null-device setting on page 656](#)
- [config log setting on page 657](#)
- [config log syslogd2 filter on page 679](#)
- [config log syslogd2 override-filter on page 682](#)
- [config log syslogd2 override-setting on page 686](#)
- [config log syslogd2 setting on page 691](#)
- [config log syslogd3 filter on page 696](#)

- [config log syslogd3 override-filter on page 700](#)
- [config log syslogd3 override-setting on page 703](#)
- [config log syslogd3 setting on page 708](#)
- [config log syslogd4 filter on page 714](#)
- [config log syslogd4 override-filter on page 717](#)
- [config log syslogd4 override-setting on page 721](#)
- [config log syslogd4 setting on page 726](#)
- [config log syslogd filter on page 661](#)
- [config log syslogd override-filter on page 665](#)
- [config log syslogd override-setting on page 669](#)
- [config log syslogd setting on page 674](#)
- [config log tacacs+accounting2 filter on page 733](#)
- [config log tacacs+accounting2 setting on page 734](#)
- [config log tacacs+accounting3 filter on page 735](#)
- [config log tacacs+accounting3 setting on page 736](#)
- [config log tacacs+accounting filter on page 731](#)
- [config log tacacs+accounting setting on page 732](#)
- [config log threat-weight on page 737](#)
- [config log webtrends filter on page 749](#)
- [config log webtrends setting on page 752](#)

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 severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    set forti-switch [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
end
```

config log disk filter

Parameter	Description	Type	Size	Default
severity	Log to disk 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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>debug</i>	Debug level.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Traffic log.</td></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></table>	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.			
	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.																																							
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.																																							

config log disk setting

Settings for local disk logging.

```
config log disk setting
  Description: Settings for local disk logging.
  set status [enable|disable]
  set ips-archive [enable|disable]
```

```

set max-log-file-size {integer}
set max-policy-packet-capture-size {integer}
set roll-schedule [daily|weekly]
set roll-day {option1}, {option2}, ...
set roll-time {user}
set diskfull [overwrite|nolog]
set log-quota {integer}
set dlp-archive-quota {integer}
set report-quota {integer}
set maximum-log-age {integer}
set upload [enable|disable]
set upload-destination {option}
set uploadip {ipv4-address}
set uploadport {integer}
set source-ip {ipv4-address}
set uploaduser {string}
set uploadpass {password}
set uploaddir {string}
set uploadtype {option1}, {option2}, ...
set uploadsched [disable|enable]
set uploadtime {user}
set upload-delete-files [enable|disable]
set upload-ssl-conn [default|high|...]
set full-first-warning-threshold {integer}
set full-second-warning-threshold {integer}
set full-final-warning-threshold {integer}
set interface-select-method [auto|specify]
set interface {string}
end

```

config log disk setting

Parameter	Description	Type	Size	Default						
status	Enable/disable local disk logging.	option	-	enable						
	<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.									
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archiving.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archiving.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archiving.	<i>disable</i>	Disable IPS packet archiving.			
Option	Description									
<i>enable</i>	Enable IPS packet archiving.									
<i>disable</i>	Disable IPS packet archiving.									

Parameter	Description	Type	Size	Default																
max-log-file-size	Maximum log file size before rolling (1 - 100 Mbytes).	integer	Minimum value: 1 Maximum value: 100	20																
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100																
roll-schedule	Frequency to check log file for rolling.	option	-	daily																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Check the log file once a day.</td></tr><tr><td>weekly</td><td>Check the log file once a week.</td></tr></table>				Option	Description	daily	Check the log file once a day.	weekly	Check the log file once a week.										
Option	Description																			
daily	Check the log file once a day.																			
weekly	Check the log file once a week.																			
roll-day	Day of week on which to roll log file.	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																			
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified																	
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>overwrite</td><td>Overwrite the oldest logs when the log disk is full.</td></tr><tr><td>nolog</td><td>Stop logging when the log disk is full.</td></tr></table>				Option	Description	overwrite	Overwrite the oldest logs when the log disk is full.	nolog	Stop logging when the log disk is full.										
Option	Description																			
overwrite	Overwrite the oldest logs when the log disk is full.																			
nolog	Stop logging when the log disk is full.																			

Parameter	Description	Type	Size	Default						
log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0						
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0						
report-quota	Report db quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0						
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7						
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-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.									
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0						
uploadport	TCP port to use for communicating with the FTP server (default = 21).	integer	Minimum value: 0 Maximum value: 65535	21						
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified	
uploadaddr	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	
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

Option	Description
<i>traffic</i>	Upload traffic log.
<i>event</i>	Upload event log.
<i>virus</i>	Upload anti-virus log.
<i>webfilter</i>	Upload web filter log.
<i>IPS</i>	Upload IPS log.
<i>emailfilter</i>	Upload spam filter log.
<i>dlp-archive</i>	Upload DLP archive.
<i>anomaly</i>	Upload anomaly log.
<i>voip</i>	Upload VoIP log.
<i>dlp</i>	Upload DLP log.
<i>app-ctrl</i>	Upload application control log.
<i>waf</i>	Upload web application firewall log.
<i>dns</i>	Upload DNS log.
<i>ssh</i>	Upload SSH log.
<i>ssl</i>	Upload SSL log.
<i>file-filter</i>	Upload file-filter log.
<i>icap</i>	Upload ICAP log.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>virtual-patch</i>	Upload virtual-patch log.		
uploadsched	Set the schedule for uploading log files to the FTP server (default = disable = upload when rolling).	option	-	disable
	Option	Description		
	<i>disable</i>	Upload when rolling.		
	<i>enable</i>	Scheduled upload.		
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified	
upload-delete-files	Delete log files after uploading (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Delete log files after uploading.		
	<i>disable</i>	Do not delete log files after uploading.		
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default
	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.		
full-first-warning-threshold	Log full first warning threshold as a percent (1 - 98, default = 75).	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent (2 - 99, default = 90).	integer	Minimum value: 2 Maximum value: 99	90

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
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log eventfilter

Configure log event filters.

```

config log eventfilter
    Description: Configure log event filters.
    set event [enable|disable]
    set system [enable|disable]
    set vpn [enable|disable]
    set user [enable|disable]
    set router [enable|disable]
    set wireless-activity [enable|disable]
    set wan-opt [enable|disable]
    set endpoint [enable|disable]
    set ha [enable|disable]
    set security-rating [enable|disable]
    set fortiextender [enable|disable]
    set connector [enable|disable]
    set sdwan [enable|disable]
    set cifs [enable|disable]
    set switch-controller [enable|disable]
    set wcs [enable|disable]
    set wdb [enable|disable]
    set aggd [enable|disable]
    set crwl [enable|disable]
    set rest-api [enable|disable]
    set webproxy [enable|disable]
    set iptables [enable|disable]
end

```

config log eventfilter

Parameter	Description	Type	Size	Default						
event	Enable/disable event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable event logging.</td></tr><tr><td><i>disable</i></td><td>Disable event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable event logging.	<i>disable</i>	Disable event logging.			
Option	Description									
<i>enable</i>	Enable event logging.									
<i>disable</i>	Disable event logging.									
system	Enable/disable system event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable system event logging.</td></tr><tr><td><i>disable</i></td><td>Disable system event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable system event logging.	<i>disable</i>	Disable system event logging.			
Option	Description									
<i>enable</i>	Enable system event logging.									
<i>disable</i>	Disable system event logging.									
vpn	Enable/disable VPN event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VPN event logging.</td></tr><tr><td><i>disable</i></td><td>Disable VPN event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VPN event logging.	<i>disable</i>	Disable VPN event logging.			
Option	Description									
<i>enable</i>	Enable VPN event logging.									
<i>disable</i>	Disable VPN event logging.									
user	Enable/disable user authentication event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user authentication event logging.</td></tr><tr><td><i>disable</i></td><td>Disable user authentication event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable user authentication event logging.	<i>disable</i>	Disable user authentication event logging.			
Option	Description									
<i>enable</i>	Enable user authentication event logging.									
<i>disable</i>	Disable user authentication event logging.									
router	Enable/disable router event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable router event logging.</td></tr><tr><td><i>disable</i></td><td>Disable router event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable router event logging.	<i>disable</i>	Disable router event logging.			
Option	Description									
<i>enable</i>	Enable router event logging.									
<i>disable</i>	Disable router event logging.									
wireless-activity	Enable/disable wireless event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless event logging.</td></tr><tr><td><i>disable</i></td><td>Disable wireless event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable wireless event logging.	<i>disable</i>	Disable wireless event logging.			
Option	Description									
<i>enable</i>	Enable wireless event logging.									
<i>disable</i>	Disable wireless event logging.									

Parameter	Description	Type	Size	Default						
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN optimization event logging.</td></tr><tr><td><i>disable</i></td><td>Disable WAN optimization event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable WAN optimization event logging.	<i>disable</i>	Disable WAN optimization event logging.			
Option	Description									
<i>enable</i>	Enable WAN optimization event logging.									
<i>disable</i>	Disable WAN optimization event logging.									
endpoint	Enable/disable endpoint event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable endpoint event logging.</td></tr><tr><td><i>disable</i></td><td>Disable endpoint event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable endpoint event logging.	<i>disable</i>	Disable endpoint event logging.			
Option	Description									
<i>enable</i>	Enable endpoint event logging.									
<i>disable</i>	Disable endpoint event logging.									
ha	Enable/disable ha event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ha event logging.</td></tr><tr><td><i>disable</i></td><td>Disable ha event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ha event logging.	<i>disable</i>	Disable ha event logging.			
Option	Description									
<i>enable</i>	Enable ha event logging.									
<i>disable</i>	Disable ha event logging.									
security-rating	Enable/disable Security Rating result logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Security Fabric audit result logging.</td></tr><tr><td><i>disable</i></td><td>Disable Security Fabric audit result logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Security Fabric audit result logging.	<i>disable</i>	Disable Security Fabric audit result logging.			
Option	Description									
<i>enable</i>	Enable Security Fabric audit result logging.									
<i>disable</i>	Disable Security Fabric audit result logging.									
fortiextender	Enable/disable FortiExtender logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Extender logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Extender logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Extender logging.	<i>disable</i>	Disable Forti-Extender logging.			
Option	Description									
<i>enable</i>	Enable Forti-Extender logging.									
<i>disable</i>	Disable Forti-Extender logging.									
connector	Enable/disable SDN connector logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SDN connector logging.</td></tr><tr><td><i>disable</i></td><td>Disable SDN connector logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable SDN connector logging.	<i>disable</i>	Disable SDN connector logging.			
Option	Description									
<i>enable</i>	Enable SDN connector logging.									
<i>disable</i>	Disable SDN connector logging.									
sdwan	Enable/disable SD-WAN logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SD-WAN logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable SD-WAN logging.					
Option	Description									
<i>enable</i>	Enable SD-WAN logging.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable SD-WAN logging.		
cifs	Enable/disable CIFS logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable CIFS logging.		
	<i>disable</i>	Disable CIFS 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.		
wcs	Enable/disable log for wcs events.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
wdb	Enable/disable log for wdb events.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
aggd	Enable/disable log for aggd events.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
crwl	Enable/disable log for crwl events.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		

Parameter	Description	Type	Size	Default
rest-api	Enable/disable REST API logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable REST API logging.		
	<i>disable</i>	Disable REST API logging.		
webproxy	Enable/disable web proxy event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Web Proxy event logging.		
	<i>disable</i>	Disable Web Proxy event logging.		
iptables	Enable/disable iptables event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable iptables event logging.		
	<i>disable</i>	Disable iptables event logging.		

config log fortianalyzer filter

Filters for FortiAnalyzer.

```

config log fortianalyzer filter
    Description: Filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    set forti-switch [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
end
end

```

config log fortianalyzer filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option Description			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [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
end
```

config log fortianalyzer override-filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
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.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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></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.			
	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.																															
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.																															

config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
  Description: Override FortiAnalyzer settings.
  set use-management-vdom [enable|disable]
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
```

```

set server-cert-ca {string}
set preshared-key {string}
set access-config [enable|disable]
set hmac-algorithm {option}
set enc-algorithm [high-medium|high|...]
set ssl-min-proto-version [default|SSLv3|...]
set conn-timeout {integer}
set monitor-keepalive-period {integer}
set monitor-failure-retry-period {integer}
set certificate {string}
set source-ip {string}
set upload-option [store-and-upload|realtime|...]
set upload-interval [daily|weekly|...]
set upload-day {user}
set upload-time {user}
set reliable [enable|disable]
set priority [default|low]
set max-log-rate {integer}
set interface-select-method [auto|specify]
set interface {string}
end

```

config log fortianalyzer override-setting

Parameter	Description	Type	Size	Default						
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.									
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.									
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></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.					
Option	Description									
<i>enable</i>	Enable IPS packet archive logging.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable IPS packet archive logging.					
Option	Description									
<i>disable</i>	Disable IPS packet archive logging.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
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.									
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><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.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79							
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256						

Parameter	Description	Type	Size	Default											
enc-algorithm	<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	-	high						
	Option	Description													
	<i>sha256</i>	Use SHA256 as HMAC algorithm.													
	Configure the level of SSL protection for secure communication with FortiAnalyzer.														
<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.														
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>
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.														
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10											
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5											
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5											
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35												

Parameter	Description	Type	Size	Default
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	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-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	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-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
	priority	Set log transmission priority.	option	-
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		

Parameter	Description	Type	Size	Default
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer setting

Global FortiAnalyzer settings.

```
config log fortianalyzer setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set server-cert-ca {string}
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm {option}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
```

```

set interface-select-method [auto|specify]
set interface {string}
end

```

config log fortianalyzer setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
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.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable
	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.		
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.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default														
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79															
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63															
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.																	
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.																	
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.																	
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										
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10										
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5										
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35											
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63											
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-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-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											

Parameter	Description	Type	Size	Default
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
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.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer2 filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
```

```

set voip [enable|disable]
set dlp-archive [enable|disable]
set forti-switch [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
end

```

config log fortianalyzer2 filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		

Parameter	Description	Type	Size	Default						
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.									
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.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic 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.									
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.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	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.		

config free-style

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch 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.		

config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```

config log fortianalyzer2 override-filter
    Description: Override filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    set forti-switch [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
end
end

```

config log fortianalyzer2 override-filter

Parameter	Description	Type	Size	Default																		
severity	Log every message above and including this severity level.	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.																					
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.																					
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.																					
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer2 override-setting
  Description: Override FortiAnalyzer settings.
  set use-management-vdom [enable|disable]
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set server-cert-ca {string}
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm {option}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|specify]
  set interface {string}
end
```

config log fortianalyzer2 override-setting

Parameter	Description	Type	Size	Default
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option Description			
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
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.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable
	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.		
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.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default														
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79															
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63															
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
Option	Description																	
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.																	
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.																	
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.																	
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.																	
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.																	

Parameter	Description	Type	Size	Default										
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10										
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5										
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35											
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63											
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-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-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											

Parameter	Description	Type	Size	Default
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
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.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer2 setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set server-cert-ca {string}
  set preshared-key {string}
```

```

set access-config [enable|disable]
set hmac-algorithm {option}
set enc-algorithm [high-medium|high|...]
set ssl-min-proto-version [default|SSLv3|...]
set conn-timeout {integer}
set monitor-keepalive-period {integer}
set monitor-failure-retry-period {integer}
set certificate {string}
set source-ip {string}
set upload-option [store-and-upload|realtime|...]
set upload-interval [daily|weekly|...]
set upload-day {user}
set upload-time {user}
set reliable [enable|disable]
set priority [default|low]
set max-log-rate {integer}
set interface-select-method [auto|specify]
set interface {string}
end

```

config log fortianalyzer2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option Description			
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
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.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
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
	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.		
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.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
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.		
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
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														
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.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
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-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-day	Day of week (month) to upload logs.	user	Not Specified									
upload-time	Time to upload logs (hh:mm).	user	Not Specified									
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.											
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.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
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>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.					
Option	Description											
auto	Set outgoing interface automatically.											
specify	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer3 filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [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
end
```

config log fortianalyzer3 filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
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.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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></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.			
	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.																															
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.																															

config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer3 override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
```

```

set voip [enable|disable]
set dlp-archive [enable|disable]
set forti-switch [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
end

```

config log fortianalyzer3 override-filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		

Parameter	Description	Type	Size	Default						
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.									
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.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic 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.									
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.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	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.		

config free-style

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch 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.		

config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```

config log fortianalyzer3 override-setting
  Description: Override FortiAnalyzer settings.
  set use-management-vdom [enable|disable]
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set server-cert-ca {string}
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm {option}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}

```

```

set reliable [enable|disable]
set priority [default|low]
set max-log-rate {integer}
set interface-select-method [auto|specify]
set interface {string}
end

```

config log fortianalyzer3 override-setting

Parameter	Description	Type	Size	Default						
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.									
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.									
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.									
server	The remote FortiAnalyzer.	string	Maximum length: 127							
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
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.											
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><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.											
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79									
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79									
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63									
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.					
	Option	Description										
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.										
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
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.											
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.											

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.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
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-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-day	Day of week (month) to upload logs.	user	Not Specified									
upload-time	Time to upload logs (hh:mm).	user	Not Specified									
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.											
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.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
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>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.					
Option	Description											
auto	Set outgoing interface automatically.											
specify	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer3 setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set server-cert-ca {string}
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm {option}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set reliable [enable|disable]
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|specify]
  set interface {string}
end
```

config log fortianalyzer3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable
	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.		
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.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
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.		
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256

Parameter	Description	Type	Size	Default														
enc-algorithm	<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	-	high										
	Option	Description																
	sha256	Use SHA256 as HMAC algorithm.																
	Configure the level of SSL protection for secure communication with FortiAnalyzer.																	
	<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.																	
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.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															

Parameter	Description	Type	Size	Default										
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63											
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-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-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
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.													
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.													

Parameter	Description	Type	Size	Default						
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```

config log fortianalyzer-cloud filter
  Description: Filters for FortiAnalyzer Cloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [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
end
end

```

config log fortianalyzer-cloud filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option Description			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud override-filter
  Description: Override filters for FortiAnalyzer Cloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  set forti-switch [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
end
```

config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
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.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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></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.			
	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.																															
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.																															

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
	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 status [enable|disable]
  set ips-archive [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm {option}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set priority [default|low]
  set max-log-rate {integer}
  set interface-select-method [auto|specify]
  set interface {string}
end
```

config log fortianalyzer-cloud 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.		
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.		
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.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
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.		
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
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.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></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</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.											
	Option	Description																
	<i>high</i>	Encrypt logs using high encryption algorithms.																
<i>low</i>	Encrypt logs using all encryption algorithms.																	
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.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor- keepalive- period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor- failure-retry- period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
upload- option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														

Parameter	Description	Type	Size	Default
	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-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	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-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
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.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortiguard filter

Filters for FortiCloud.

```
config log fortiguard filter
  Description: Filters for FortiCloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set forti-switch [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
end
```

config log fortiguard filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
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.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

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

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></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></table>	Option	Description	<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.			
	Option	Description																				
	<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.																					
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.																					

config log fortiguard override-filter

Override filters for FortiCloud.

```

config log fortiguard override-filter
  Description: Override filters for FortiCloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set forti-switch [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
end
```

config log fortiguard override-filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

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 override [enable|disable]
  set status [enable|disable]
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
  set priority [default|low]
  set max-log-rate {integer}
  set access-config [enable|disable]
end
```

config log fortiguard override-setting

Parameter	Description	Type	Size	Default
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override FortiCloud logging settings.		
	<i>disable</i>	Use global FortiCloud logging settings.		
status	Enable/disable logging to FortiCloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
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.		

Parameter	Description	Type	Size	Default
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	Option Description			
	daily	Upload log files to FortiCloud once a day.		
	weekly	Upload log files to FortiCloud once a week.		
	monthly	Upload log files to FortiCloud once a month.		
upload-day	Day of week to roll logs.	user	Not Specified	
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	
priority	Set log transmission priority.	option	-	default
	Option Description			
	default	Set FortiCloud log transmission priority to default.		
	low	Set FortiCloud log transmission priority to low.		
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable
	Option Description			
	enable	Enable FortiCloud access to configuration and data.		
	disable	Disable FortiCloud access to configuration and data.		

config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
  Description: Configure logging to FortiCloud.
  set status [enable|disable]
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
  set upload-time {user}
```



```

set priority [default|low]
set max-log-rate {integer}
set access-config [enable|disable]
set enc-algorithm [high-medium|high|...]
set ssl-min-proto-version [default|SSLv3|...]
set conn-timeout {integer}
set source-ip {ipv4-address}
set interface-select-method [auto|specify]
set interface {string}
end

```

config log fortiguard setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiCloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
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-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-day	Day of week to roll logs.	user	Not Specified	
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	

Parameter	Description	Type	Size	Default														
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.																	
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
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.																	
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.																	
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						
conn-timeout	FortiProxy Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600	10						
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified	0.0.0.0						
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>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.
	Option	Description								
	auto	Set outgoing interface automatically.								
specify	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

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 resolve-hosts [enable|disable]
    set resolve-apps [enable|disable]
    set fortiview-unscanned-apps [enable|disable]
end
```

config log gui-display

Parameter	Description	Type	Size	Default						
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable resolving IP addresses to hostnames.</td></tr><tr><td><i>disable</i></td><td>Disable resolving IP addresses to hostnames.</td></tr></table>				Option	Description	<i>enable</i>	Enable resolving IP addresses to hostnames.	<i>disable</i>	Disable resolving IP addresses to hostnames.
Option	Description									
<i>enable</i>	Enable resolving IP addresses to hostnames.									
<i>disable</i>	Disable resolving IP addresses to hostnames.									

Parameter	Description	Type	Size	Default
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.		
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable showing unscanned traffic.		
	<i>disable</i>	Disable showing unscanned traffic.		

config log memory filter

Filters for memory buffer.

```

config log memory filter
    Description: Filters for memory buffer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set forti-switch [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
end
end

```

config log memory filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log memory global-setting

Global settings for memory logging.

```
config log memory global-setting
  Description: Global settings for memory logging.
  set max-size {integer}
  set full-first-warning-threshold {integer}
  set full-second-warning-threshold {integer}
  set full-final-warning-threshold {integer}
end
```

config log memory global-setting

Parameter	Description	Type	Size	Default
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295	41299517
full-first-warning-threshold	Log full first warning threshold as a percent (1 - 98, default = 75).	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent (2 - 99, default = 90).	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent (3 - 100, default = 95).	integer	Minimum value: 3 Maximum value: 100	95

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 FortiProxy's memory.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to memory.		
	<i>disable</i>	Disable logging to memory.		

config log null-device filter

Filters for null device logging.

```
config log null-device filter
  Description: Filters for null device logging.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set forti-switch [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
end
```

config log null-device filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Traffic log.</td></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></table>	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.			
	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.																																							
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.																																							

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
		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 resolve-ip [enable|disable]
  set resolve-port [enable|disable]
  set log-user-in-upper [enable|disable]
  set fwpolicy-implicit-log [enable|disable]
  set fwpolicy6-implicit-log [enable|disable]
  set extended-log [enable|disable]
  set local-in-allow [enable|disable]
  set local-in-deny-unicast [enable|disable]
  set local-in-deny-broadcast [enable|disable]
  set local-out [enable|disable]
  set local-out-ioc-detection [enable|disable]
  set daemon-log [enable|disable]
  set neighbor-event [enable|disable]
  set brief-traffic-format [enable|disable]
  set user-anonymize [enable|disable]
  set expolicy-implicit-log [enable|disable]
  set log-policy-comment [enable|disable]
  set faz-override [enable|disable]
  set syslog-override [enable|disable]
  set rest-api-set [enable|disable]
  set rest-api-get [enable|disable]
  set long-live-session-stat [enable|disable]
  set custom-log-fields <field-id1>, <field-id2>, ...
  set anonymization-hash {string}
end
```

config log setting

Parameter	Description	Type	Size	Default						
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding resolved domain names to traffic logs.</td></tr><tr><td><i>disable</i></td><td>Disable adding resolved domain names to traffic logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding resolved domain names to traffic logs.	<i>disable</i>	Disable adding resolved domain names to traffic logs.			
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding resolved service names to traffic logs.</td></tr><tr><td><i>disable</i></td><td>Disable adding resolved service names to traffic logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding resolved service names to traffic logs.	<i>disable</i>	Disable adding resolved service names to traffic logs.			
Option	Description									
<i>enable</i>	Enable adding resolved service names to traffic logs.									
<i>disable</i>	Disable adding resolved service names to traffic logs.									
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logs with user-in-upper.</td></tr><tr><td><i>disable</i></td><td>Disable logs with user-in-upper.</td></tr></table>	Option	Description	<i>enable</i>	Enable logs with user-in-upper.	<i>disable</i>	Disable logs with user-in-upper.			
Option	Description									
<i>enable</i>	Enable logs with user-in-upper.									
<i>disable</i>	Disable logs with user-in-upper.									
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable implicit firewall policy logging.</td></tr><tr><td><i>disable</i></td><td>Disable implicit firewall policy logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable implicit firewall policy logging.	<i>disable</i>	Disable implicit firewall policy logging.			
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable implicit firewall policy6 logging.</td></tr><tr><td><i>disable</i></td><td>Disable implicit firewall policy6 logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable implicit firewall policy6 logging.	<i>disable</i>	Disable implicit firewall policy6 logging.			
Option	Description									
<i>enable</i>	Enable implicit firewall policy6 logging.									
<i>disable</i>	Disable implicit firewall policy6 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></table>	Option	Description	<i>enable</i>	Enable extended traffic logging.					
Option	Description									
<i>enable</i>	Enable extended traffic logging.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable extended traffic 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-unicast	Enable/disable local-in-deny-unicast logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local-in-deny-unicast logging.		
	<i>disable</i>	Disable local-in-deny-unicast 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-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.		
daemon-log	Enable/disable daemon logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable daemon logging.		
	<i>disable</i>	Disable daemon 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.		
brief-traffic-format	Enable/disable brief format traffic logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable brief format traffic logging.		
	<i>disable</i>	Disable brief format traffic logging.		
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.		
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable explicit proxy firewall implicit policy logging.		
	<i>disable</i>	Disable explicit proxy firewall implicit policy logging.		
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.		
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.		
syslog-override	Enable/disable override Syslog settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable override Syslog settings.		
	<i>disable</i>	Disable override Syslog settings.		
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.		
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.		
long-live-session-stat	Enable/disable long-live-session statistics logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable long-live-session statistics logging.		
	<i>disable</i>	Disable long-live-session statistics logging.		
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35	
anonymization-hash	User name anonymization hash salt.	string	Maximum length: 32	

config log syslogd filter

Filters for remote system server.

```

config log syslogd filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set forti-switch [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
end

```

config log syslogd filter

Parameter	Description	Type	Size	Default
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.		
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.		

Parameter	Description	Type	Size	Default						
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.									
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.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic 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.									
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.									
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.		
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.		

config free-style

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch 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.		

config log syslogd override-filter

Override filters for remote system server.

```

config log syslogd override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set forti-switch [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
end
end

```

config log syslogd override-filter

Parameter	Description	Type	Size	Default																		
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.																					
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.																					
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.																					
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

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

config log syslogd override-setting

Override settings for remote syslog server.

```
config log syslogd override-setting
  Description: Override settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|specify]
  set interface {string}
  config log-templates
    Description: Custom log templates.
    edit <id>
      set category [traffic|event|...]
      set empty-value-indicator {string}
      set template {string}
    next
  end
end
```

config log syslogd override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

Parameter	Description	Type	Size	Default
server	Address of remote syslog server.	string	Maximum length: 127	
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
facility	Remote syslog facility.	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 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.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></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>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>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.																							
source-ip	Source IP address of syslog.	string	Maximum length: 63																					
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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																						
<i>custom</i>	Custom format.																							
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.																							
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0																				
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.																	
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.											
	Option	Description																
	<i>auto</i>	Set outgoing interface automatically.																
<i>specify</i>	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config custom-field-name

Parameter	Description	Type	Size	Default
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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.			

Parameter	Description	Type	Size	Default
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd setting

Global settings for remote syslog server.

```

config log syslogd setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end
end

```

config log syslogd setting

Parameter	Description	Type	Size	Default																						
status	Enable/disable remote syslog logging.	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.																									
server	Address of remote syslog server.	string	Maximum length: 127																							
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).																									
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																						
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></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.			
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.																									

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></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>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>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.																																	
source-ip	Source IP address of syslog.	string	Maximum length: 63																															
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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																																
<i>custom</i>	Custom format.																																	
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.																																	

Parameter	Description	Type	Size	Default														
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<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.																	
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.											
Option	Description																	
<i>auto</i>	Set outgoing interface automatically.																	
<i>specify</i>	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config custom-field-name

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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch log.		
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd2 filter

Filters for remote system server.

```

config log syslogd2 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set forti-switch [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
end
end

```

config log syslogd2 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

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.																				
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.																					
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.																					
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.																					
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default
	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.		
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.		

config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
```

```

set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set sniffer-traffic [enable|disable]
set ztna-traffic [enable|disable]
set http-transaction [enable|disable]
set anomaly [enable|disable]
set voip [enable|disable]
set forti-switch [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
end

```

config log syslogd2 override-filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly 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.		
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.		

config free-style

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>virtual-patch</i>	Virtual patch 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.		

config log syslogd2 override-setting

Override settings for remote syslog server.

```
config log syslogd2 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
```

```

edit <id>
    set category [traffic|event|...]
    set empty-value-indicator {string}
    set template {string}
next
end
end

```

config log syslogd2 override-setting

Parameter	Description	Type	Size	Default										
status	Enable/disable remote syslog logging.	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.													
server	Address of remote syslog server.	string	Maximum length: 127											
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).													
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514										
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></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.			
Option	Description													
<i>kernel</i>	Kernel messages.													
<i>user</i>	Random user-level messages.													
<i>mail</i>	Mail system.													
<i>daemon</i>	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.																																														
source-ip	Source IP address of syslog.	string	Maximum length: 63																																												
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></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.																																			
	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.																																														

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.											
	Option	Description																
	<i>json</i>	JSON (JavaScript Object Notation) format.																
<i>custom</i>	Custom format.																	
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.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<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.																	
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default										
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
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></table>				Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.
	Option	Description												
	traffic	Traffic log.												
	event	Event log.												
	virus	Antivirus log.												
webfilter	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></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.			
	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.																															
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1																													
template	Log template string.	string	Maximum length: 2047																													

config log syslogd2 setting

Global settings for remote syslog server.

```
config log syslogd2 setting
  Description: Global settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
```

```

config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
        set name {string}
        set custom {string}
    next
end
set interface-select-method [auto|specify]
set interface {string}
config log-templates
    Description: Custom log templates.
    edit <id>
        set category [traffic|event|...]
        set empty-value-indicator {string}
        set template {string}
    next
end
end

```

config log syslogd2 setting

Parameter	Description	Type	Size	Default								
status	Enable/disable remote syslog logging.	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.											
server	Address of remote syslog server.	string	Maximum length: 127									
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).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								

Parameter	Description	Type	Size	Default
facility	Remote syslog facility.	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 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.			
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default

Parameter	Description	Type	Size	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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																
<i>custom</i>	Custom format.																	
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.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<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.																	
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></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.							
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
<i>TLSv1-1</i>	TLSv1.1.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Traffic log.</td></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></table>	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.			
	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.																																							
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1																																					
template	Log template string.	string	Maximum length: 2047																																					

config log syslogd3 filter

Filters for remote system server.

```
config log syslogd3 filter
  Description: Filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
```

```

set ztna-traffic [enable|disable]
set http-transaction [enable|disable]
set anomaly [enable|disable]
set voip [enable|disable]
set forti-switch [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
end

```

config log syslogd3 filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		

Parameter	Description	Type	Size	Default						
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.									
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.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic 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.									
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.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP 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.		

config free-style

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

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
		Option	Description	
		<i>include</i>	Include logs that match the filter.	
		<i>exclude</i>	Exclude logs that match the filter.	

config log syslogd3 override-filter

Override filters for remote system server.

```

config log syslogd3 override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set forti-switch [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
end
end

```

config log syslogd3 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
		Option	Description	
		<i>emergency</i>	Emergency level.	

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></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>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>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.																			
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.																			
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.																			
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.																			
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Traffic log.</td></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></table>	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.			
	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.																																							
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.																																							

config log syslogd3 override-setting

Override settings for remote syslog server.

```
config log syslogd3 override-setting
  Description: Override settings for remote syslog server.
  set status [enable|disable]
  set server {string}
```

```

set mode [udp|legacy-reliable|...]
set port {integer}
set facility [kernel|user|...]
set source-ip {string}
set format [default|csv|...]
set priority [default|low]
set max-log-rate {integer}
set enc-algorithm [high-medium|high|...]
set ssl-min-proto-version [default|SSLv3|...]
set certificate {string}
config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
        set name {string}
        set custom {string}
    next
end
set interface-select-method [auto|specify]
set interface {string}
config log-templates
    Description: Custom log templates.
    edit <id>
        set category [traffic|event|...]
        set empty-value-indicator {string}
        set template {string}
    next
end
end

```

config log syslogd3 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option Description			
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	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																																								
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></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.			
	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.																																											

Parameter	Description	Type	Size	Default															
	<table><tr><th>Option</th><th>Description</th></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>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>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.																	
source-ip	Source IP address of syslog.	string	Maximum length: 63																
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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																	
<i>custom</i>	Custom format.																		
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.																		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0															
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable															
	<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></table>		Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.											
	Option	Description																	
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																	
<i>high</i>	SSL communication with high encryption algorithms.																		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></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>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.											
	Option	Description																
	<i>low</i>	SSL communication with low encryption algorithms.																
<i>disable</i>	Disable SSL communication.																	
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.											
	Option	Description																
	<i>auto</i>	Set outgoing interface automatically.																
<i>specify</i>	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config custom-field-name

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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.			
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd3 setting

Global settings for remote syslog server.


```

config log syslogd3 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
        set name {string}
        set custom {string}
    next
end
set interface-select-method [auto|specify]
set interface {string}
config log-templates
    Description: Custom log templates.
    edit <id>
        set category [traffic|event|...]
        set empty-value-indicator {string}
        set template {string}
    next
end
end

```

config log syslogd3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Parameter	Description	Type	Size	Default																																						
	<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).																																									
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																																						
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></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.			
	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.																																									

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.																	
source-ip	Source IP address of syslog.	string	Maximum length: 63															
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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																
<i>custom</i>	Custom format.																	
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.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<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></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.													
	Option	Description																
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></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</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</i>	SSL communication with high encryption algorithms.																
	<i>low</i>	SSL communication with low encryption algorithms.																
	<i>disable</i>	Disable SSL communication.																
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.											
	Option	Description																
	<i>auto</i>	Set outgoing interface automatically.																
<i>specify</i>	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config custom-field-name

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	

Parameter	Description	Type	Size	Default
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.			
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd4 filter

Filters for remote system server.

```
config log syslogd4 filter
  Description: Filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set forti-switch [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
end
```

config log syslogd4 filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
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.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

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

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></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></table>	Option	Description	<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.			
	Option	Description																				
	<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.																					
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.																					

config log syslogd4 override-filter

Override filters for remote system server.

```

config log syslogd4 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set forti-switch [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
end
```

config log syslogd4 override-filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log syslogd4 override-setting

Override settings for remote syslog server.

```
config log syslogd4 override-setting
  Description: Override settings for remote syslog server.
  set status [enable|disable]
  set server {string}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set facility [kernel|user|...]
  set source-ip {string}
  set format [default|csv|...]
  set priority [default|low]
  set max-log-rate {integer}
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set interface-select-method [auto|specify]
  set interface {string}
  config log-templates
    Description: Custom log templates.
    edit <id>
      set category [traffic|event|...]
      set empty-value-indicator {string}
      set template {string}
    next
  end
end
```

config log syslogd4 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

Parameter	Description	Type	Size	Default
server	Address of remote syslog server.	string	Maximum length: 127	
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
facility	Remote syslog facility.	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 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.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></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>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>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.																							
source-ip	Source IP address of syslog.	string	Maximum length: 63																					
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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																						
<i>custom</i>	Custom format.																							
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.																							
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0																				
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.																	
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.											
	Option	Description																
	<i>auto</i>	Set outgoing interface automatically.																
<i>specify</i>	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config custom-field-name

Parameter	Description	Type	Size	Default
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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.			

Parameter	Description	Type	Size	Default
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd4 setting

Global settings for remote syslog server.

```

config log syslogd4 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end

```

config log syslogd4 setting

Parameter	Description	Type	Size	Default																						
status	Enable/disable remote syslog logging.	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.																									
server	Address of remote syslog server.	string	Maximum length: 127																							
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).																									
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																						
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></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.			
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.																									

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></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>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>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.																																	
source-ip	Source IP address of syslog.	string	Maximum length: 63																															
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><tr><td><i>custom</i></td><td>Custom 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.	<i>custom</i>	Custom 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.																																
<i>custom</i>	Custom format.																																	
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.																																	

Parameter	Description	Type	Size	Default														
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
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.																	
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.																	
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35															
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>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.											
Option	Description																	
auto	Set outgoing interface automatically.																	
specify	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config custom-field-name

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	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	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.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></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></table>				Option	Description	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.	<i>virtual-patch</i>	Virtual patch log.
	Option	Description										
	<i>file-filter</i>	File filter log.										
	<i>icap</i>	ICAP log.										
<i>virtual-patch</i>	Virtual patch log.											
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1									
template	Log template string.	string	Maximum length: 2047									

config log tacacs+accounting filter

Settings for TACACS+ accounting events filter.

```

config log tacacs+accounting filter
    Description: Settings for TACACS+ accounting events filter.
    set login-audit [enable|disable]
    set config-change-audit [enable|disable]
    set cli-cmd-audit [enable|disable]
end

```

config log tacacs+accounting filter

Parameter	Description	Type	Size	Default						
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for login events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for login events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for login events audit.	<i>disable</i>	Disable TACACS+ accounting for login events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for login events audit.									
<i>disable</i>	Disable TACACS+ accounting for login events 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></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.					
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.		
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.		
	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.		

config log tacacs+accounting setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting setting
  Description: Settings for TACACS+ accounting.
  set status [enable|disable]
  set server {string}
  set server-key {password}
  set source-ip {string}
  set interface-select-method [auto|specify]
  set interface {string}
end
```

config log tacacs+accounting setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option Description			
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		
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							
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config log tacacs+accounting2 filter

Settings for TACACS+ accounting events filter.

```

config log tacacs+accounting2 filter
  Description: Settings for TACACS+ accounting events filter.
  set login-audit [enable|disable]
  set config-change-audit [enable|disable]
  set cli-cmd-audit [enable|disable]
end

```

config log tacacs+accounting2 filter

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option	Description		
	enable	Enable TACACS+ accounting for login events audit.		
	disable	Disable TACACS+ accounting for login events audit.		
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.		
	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.		
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.		
	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.		

config log tacacs+accounting2 setting

Settings for TACACS+ accounting.

```

config log tacacs+accounting2 setting
  Description: Settings for TACACS+ accounting.
  set status [enable|disable]
  set server {string}
  set server-key {password}
  set source-ip {string}
  set interface-select-method [auto|specify]
  set interface {string}
end

```

config log tacacs+accounting2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		
server	Address of TACACS+ server.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
server-key	Key to access the TACACS+ server.	password	Not Specified							
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63							
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config log tacacs+accounting3 filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting3 filter
  Description: Settings for TACACS+ accounting events filter.
  set login-audit [enable|disable]
  set config-change-audit [enable|disable]
  set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting3 filter

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-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.		
	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.		
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.		
	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.		

config log tacacs+accounting3 setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting3 setting
  Description: Settings for TACACS+ accounting.
  set status [enable|disable]
  set server {string}
  set server-key {password}
  set source-ip {string}
  set interface-select-method [auto|specify]
  set interface {string}
end
```

config log tacacs+accounting3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		
server	Address of TACACS+ server.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
server-key	Key to access the TACACS+ server.	password	Not Specified	
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log threat-weight

Configure threat weight settings.

```

config log threat-weight
  Description: Configure threat weight settings.
  set status [enable|disable]
  config level
    Description: Score mapping for threat weight levels.
    set low {integer}
    set medium {integer}
    set high {integer}
    set critical {integer}
  end
  set blocked-connection [disable|low|...]
  set failed-connection [disable|low|...]
  set url-block-detected [disable|low|...]
  set botnet-connection-detected [disable|low|...]
  config malware
    Description: Anti-virus malware threat weight settings.
    set virus-infected [disable|low|...]
    set inline-block [disable|low|...]
    set file-blocked [disable|low|...]
    set command-blocked [disable|low|...]
    set oversized [disable|low|...]
    set virus-scan-error [disable|low|...]
    set switch-proto [disable|low|...]
    set mimefragmented [disable|low|...]
    set virus-file-type-executable [disable|low|...]
    set virus-outbreak-prevention [disable|low|...]

```

```

    set content-disarm [disable|low|...]
    set malware-list [disable|low|...]
    set ems-threat-feed [disable|low|...]
    set fsa-malicious [disable|low|...]
    set fsa-high-risk [disable|low|...]
    set fsa-medium-risk [disable|low|...]
end
config ips
    Description: IPS threat weight settings.
    set info-severity [disable|low|...]
    set low-severity [disable|low|...]
    set medium-severity [disable|low|...]
    set high-severity [disable|low|...]
    set critical-severity [disable|low|...]
end
config web
    Description: Web filtering threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
config geolocation
    Description: Geolocation-based threat weight settings.
    edit <id>
        set country {string}
        set level [disable|low|...]
    next
end
config application
    Description: Application-control threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
end
end

```

config log threat-weight

Parameter	Description	Type	Size	Default
status	Enable/disable the threat weight feature.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the threat weight feature.		
	<i>disable</i>	Disable the threat weight feature.		

Parameter	Description	Type	Size	Default												
blocked-connection	Threat weight score for blocked connections.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for blocked connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for blocked connections.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for blocked connections.</td></tr><tr><td><i>high</i></td><td>Use the high level score for blocked connections.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for blocked connections.</td></tr></table>	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.	<i>high</i>	Use the high level score for blocked connections.	<i>critical</i>	Use the critical level score for blocked connections.			
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.															
<i>high</i>	Use the high level score for blocked connections.															
<i>critical</i>	Use the critical level score for blocked connections.															
failed-connection	Threat weight score for failed connections.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for failed connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for failed connections.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for failed connections.</td></tr><tr><td><i>high</i></td><td>Use the high level score for failed connections.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for failed connections.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for failed connections.	<i>low</i>	Use the low level score for failed connections.	<i>medium</i>	Use the medium level score for failed connections.	<i>high</i>	Use the high level score for failed connections.	<i>critical</i>	Use the critical level score for failed connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for failed connections.															
<i>low</i>	Use the low level score for failed connections.															
<i>medium</i>	Use the medium level score for failed connections.															
<i>high</i>	Use the high level score for failed connections.															
<i>critical</i>	Use the critical level score for failed connections.															
url-block-detected	Threat weight score for URL blocking.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for URL blocking.</td></tr><tr><td><i>low</i></td><td>Use the low level score for URL blocking.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for URL blocking.</td></tr><tr><td><i>high</i></td><td>Use the high level score for URL blocking.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for URL blocking.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for URL blocking.	<i>low</i>	Use the low level score for URL blocking.	<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.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for URL blocking.															
<i>low</i>	Use the low level score for URL blocking.															
<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.															
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for detected botnet connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for detected botnet connections.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for detected botnet connections.	<i>low</i>	Use the low level score for detected botnet connections.									
Option	Description															
<i>disable</i>	Disable threat weight scoring for detected botnet connections.															
<i>low</i>	Use the low level score for detected botnet connections.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>medium</i>	Use the medium level score for detected botnet connections.		
	<i>high</i>	Use the high level score for detected botnet connections.		
	<i>critical</i>	Use the critical level score for detected botnet connections.		

config level

Parameter	Description	Type	Size	Default
low	Low level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	5
medium	Medium level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	10
high	High level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	30
critical	Critical level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100	50

config malware

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.		

Parameter	Description	Type	Size	Default												
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.															
file-blocked	Threat weight score for blocked file detected.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for blocked file detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for blocked file detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for blocked file detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for blocked file detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for blocked file detected.</td></tr></table>	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.			
	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.															
command-blocked	Threat weight score for blocked command detected.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for blocked command detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for blocked command detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for blocked command detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for blocked command detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for blocked command detected.</td></tr></table>	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.			
	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.															
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></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for oversized file detected.											
	Option	Description														
<i>disable</i>	Disable threat weight scoring for oversized file detected.															

Parameter	Description	Type	Size	Default
	Option Description			
	<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.		
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.		
switch-proto	Threat weight score for switch proto detected.	option	-	disable
	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.		
mimefragmented	Threat weight score for mimefragmented detected.	option	-	disable
	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.		

Parameter	Description	Type	Size	Default												
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.															
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (outbreak prevention) event.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (outbreak prevention) event.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (outbreak prevention) event.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (outbreak prevention) event.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (outbreak prevention) event.</td></tr></table>	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.			
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.															
content-disarm	Threat weight score for virus (content disarm) 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 (content disarm) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (content disarm) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (content disarm) detected.</td></tr></table>	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.							
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.															

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 virus (content disarm) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (content disarm) detected.</td></tr></table>	Option	Description	<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.									
Option	Description															
<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.															
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.															
ems-threat-feed	Threat weight score for virus (EMS threat feed) 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 (EMS threat feed) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (EMS threat feed) detected.</td></tr></table>	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.			
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.															
fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox malicious malware detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox malicious malware detected.</td></tr></table>	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.									
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.															

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox malicious malware detected.</td></tr></table>	Option	Description	<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.							
	Option	Description														
	<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.															
fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox high risk malware detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox high risk malware detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox high risk malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox high risk malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox high risk malware detected.</td></tr></table>	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.			
	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-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.															

config ips

Parameter	Description	Type	Size	Default												
info-severity	Threat weight score for IPS info severity events.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for IPS info severity events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for IPS info severity events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for IPS info severity events.</td></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>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.	<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>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.															
<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.															
high-severity	Threat weight score for IPS high severity events.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for IPS high severity events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for IPS high severity events.</td></tr></table>	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.									
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.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		

config web

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255	0
level	Threat weight score for web category filtering matches.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for web category filtering matches.		
	<i>low</i>	Use the low level score for web category filtering matches.		
	<i>medium</i>	Use the medium level score for web category filtering matches.		
	<i>high</i>	Use the high level score for web category filtering matches.		
	<i>critical</i>	Use the critical level score for web category filtering matches.		

config geolocation

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
country	Country code.	string	Maximum length: 2	
level	Threat weight score for Geolocation-based events.	option	-	low
	Option	Description		
	disable	Disable threat weight scoring for Geolocation-based events.		
	low	Use the low level score for Geolocation-based events.		
	medium	Use the medium level score for Geolocation-based events.		
	high	Use the high level score for Geolocation-based events.		
	critical	Use the critical level score for Geolocation-based events.		

config application

Parameter	Description	Type	Size	Default												
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0												
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0												
level	Threat weight score for Application events.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for Application events.</td></tr><tr><td>low</td><td>Use the low level score for Application events.</td></tr><tr><td>medium</td><td>Use the medium level score for Application events.</td></tr><tr><td>high</td><td>Use the high level score for Application events.</td></tr><tr><td>critical</td><td>Use the critical level score for Application events.</td></tr></table>				Option	Description	disable	Disable threat weight scoring for Application events.	low	Use the low level score for Application events.	medium	Use the medium level score for Application events.	high	Use the high level score for Application events.	critical	Use the critical level score for Application events.
	Option	Description														
	disable	Disable threat weight scoring for Application events.														
	low	Use the low level score for Application events.														
	medium	Use the medium level score for Application events.														
	high	Use the high level score for Application events.														
critical	Use the critical level score for Application events.															

config log webtrends filter

Filters for WebTrends.

```
config log webtrends filter
  Description: Filters for WebTrends.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set forti-switch [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
end
```

config log webtrends filter

Parameter	Description	Type	Size	Default
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.		
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.		
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.		
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.		
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.		
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.		
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.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP 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.		

config free-style

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

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></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></table>	Option	Description	<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.			
	Option	Description																				
	<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.																					
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.																					

config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
    Description: Settings for WebTrends.
    set status [enable|disable]
    set server {string}
end
```

config log webtrends setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to WebTrends.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to WebTrends.</td></tr><tr><td><i>disable</i></td><td>Disble logging to WebTrends.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging to WebTrends.	<i>disable</i>	Disble logging to WebTrends.			
Option	Description									
<i>enable</i>	Enable logging to WebTrends.									
<i>disable</i>	Disble logging to WebTrends.									

Parameter	Description	Type	Size	Default
server	Address of the remote WebTrends server.	string	Maximum length: 63	

mgmt-data

This section includes syntax for the following commands:

- [config mgmt-data status on page 754](#)

config mgmt-data status

Status for mgmt-data.

```
config mgmt-data status
    Description: Status for mgmt-data.
end
```

oaas

This section includes syntax for the following commands:

- [config oaas status on page 755](#)

config oaas status

Display detailed overlay-as-a-service status.

```
config oaas status
    Description: Display detailed overlay-as-a-service status.
end
```

report

This section includes syntax for the following commands:

- [config report layout on page 756](#)
- [config report setting on page 764](#)
- [config report sql status on page 765](#)

config report layout

Report layout configuration.

```
config report layout
  Description: Report layout configuration.
  edit <name>
    set title {string}
    set subtitle {string}
    set description {string}
    set style-theme {string}
    set options {option1}, {option2}, ...
    set format {option1}, {option2}, ...
    set schedule-type [demand|daily|...]
    set day [sunday|monday|...]
    set time {user}
    set cutoff-option [run-time|custom]
    set cutoff-time {user}
    set email-send [enable|disable]
    set email-recipients {string}
    set max-pdf-report {integer}
  config page
    Description: Configure report page.
    set paper [a4|letter]
    set column-break-before {option1}, {option2}, ...
    set page-break-before {option1}, {option2}, ...
    set options {option1}, {option2}, ...
  config header
    Description: Configure report page header.
    set style {string}
  config header-item
    Description: Configure report header item.
    edit <id>
      set description {string}
      set type [text|image]
      set style {string}
      set content {string}
      set img-src {string}
```



```

        next
    end
end
config footer
    Description: Configure report page footer.
    set style {string}
    config footer-item
        Description: Configure report footer item.
        edit <id>
            set description {string}
            set type [text|image]
            set style {string}
            set content {string}
            set img-src {string}
        next
    end
end
end
config body-item
    Description: Configure report body item.
    edit <id>
        set description {string}
        set type [text|image|...]
        set style {string}
        set top-n {integer}
        config parameters
            Description: Parameters.
            edit <id>
                set name {string}
                set value {string}
            next
        end
        set text-component [text|heading1|...]
        set content {string}
        set img-src {string}
        set chart {string}
        set chart-options {option1}, {option2}, ...
        set misc-component [hline|page-break|...]
        set title {string}
    next
end
next
end
end

```

config report layout

Parameter	Description	Type	Size	Default
name	Report layout name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default												
title	Report title.	string	Maximum length: 127													
subtitle	Report subtitle.	string	Maximum length: 127													
description	Description.	string	Maximum length: 127													
style-theme	Report style theme.	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.															
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.															
schedule-type	Report schedule type.	option	-	daily												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>demand</td><td>Run on demand.</td></tr></table>				Option	Description	demand	Run on demand.								
Option	Description															
demand	Run on demand.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>daily</i>	Schedule daily.		
	<i>weekly</i>	Schedule weekly.		
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.		
time	Schedule time to generate report (format = hh:mm).	user	Not Specified	
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	
email-send	Enable/disable sending emails after reports are generated.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sending emails after generating reports.		
	<i>disable</i>	Disable sending emails after generating reports.		
email-recipients	Email recipients for generated reports.	string	Maximum length: 511	
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

config page

Parameter	Description	Type	Size	Default								
paper	Report page paper.	option	-	a4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>a4</i></td><td>A 4 paper.</td></tr><tr><td><i>letter</i></td><td>Letter paper.</td></tr></table>	Option	Description	<i>a4</i>	A 4 paper.	<i>letter</i>	Letter paper.					
Option	Description											
<i>a4</i>	A 4 paper.											
<i>letter</i>	Letter paper.											
column-break-before	Report page auto column break before heading.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>heading1</i></td><td>Column break before heading 1.</td></tr><tr><td><i>heading2</i></td><td>Column break before heading 2.</td></tr><tr><td><i>heading3</i></td><td>Column break before heading 3.</td></tr></table>	Option	Description	<i>heading1</i>	Column break before heading 1.	<i>heading2</i>	Column break before heading 2.	<i>heading3</i>	Column break before heading 3.			
Option	Description											
<i>heading1</i>	Column break before heading 1.											
<i>heading2</i>	Column break before heading 2.											
<i>heading3</i>	Column break before heading 3.											
page-break-before	Report page auto page break before heading.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>heading1</i></td><td>Page break before heading 1.</td></tr><tr><td><i>heading2</i></td><td>Page break before heading 2.</td></tr><tr><td><i>heading3</i></td><td>Page break before heading 3.</td></tr></table>	Option	Description	<i>heading1</i>	Page break before heading 1.	<i>heading2</i>	Page break before heading 2.	<i>heading3</i>	Page break before heading 3.			
Option	Description											
<i>heading1</i>	Page break before heading 1.											
<i>heading2</i>	Page break before heading 2.											
<i>heading3</i>	Page break before heading 3.											
options	Report page options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>header-on-first-page</i></td><td>Show header on first page.</td></tr><tr><td><i>footer-on-first-page</i></td><td>Show footer on first page.</td></tr></table>	Option	Description	<i>header-on-first-page</i>	Show header on first page.	<i>footer-on-first-page</i>	Show footer on first page.					
Option	Description											
<i>header-on-first-page</i>	Show header on first page.											
<i>footer-on-first-page</i>	Show footer on first page.											

config header

Parameter	Description	Type	Size	Default
style	Report header style.	string	Maximum length: 71	

config header-item

Parameter	Description	Type	Size	Default						
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
description	Description.	string	Maximum length: 63							
type	Report item type.	option	-	text						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>image</i></td><td>Image.</td></tr></table>				Option	Description	<i>text</i>	Text.	<i>image</i>	Image.
	Option	Description								
	<i>text</i>	Text.								
<i>image</i>	Image.									
style	Report item style.	string	Maximum length: 71							
content	Report item text content.	string	Maximum length: 511							
img-src	Report item image file name.	string	Maximum length: 127							

config footer

Parameter	Description	Type	Size	Default
style	Report footer style.	string	Maximum length: 71	

config footer-item

Parameter	Description	Type	Size	Default
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Text.		
	<i>image</i>	Image.		
style	Report item style.	string	Maximum length: 71	
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	

config body-item

Parameter	Description	Type	Size	Default
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text
	Option	Description		
	<i>text</i>	Text.		
	<i>image</i>	Image.		
	<i>chart</i>	Chart.		
	<i>misc</i>	Miscellaneous.		
style	Report item style.	string	Maximum length: 71	
top-n	Value of top.	integer	Minimum value: 0 Maximum value: 4294967295	0
text-component	Report item text component.	option	-	text

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Normal text.		
	<i>heading1</i>	Heading 1.		
	<i>heading2</i>	Heading 2.		
	<i>heading3</i>	Heading 3.		
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	
chart	Report item chart name.	string	Maximum length: 71	
chart-options	Report chart options.	option	-	include-no-data hide-title show-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.		
misc-component	Report item miscellaneous component.	option	-	hline
	Option	Description		
	<i>hline</i>	Horizontal line.		
	<i>page-break</i>	Page break.		
	<i>column-break</i>	Column break.		
	<i>section-start</i>	Section start.		
title	Report section title.	string	Maximum length: 511	

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 report setting

Report setting configuration.

```
config report setting
  Description: Report setting configuration.
  set pdf-report [enable|disable]
  set fortiview [enable|disable]
  set report-source {option1}, {option2}, ...
  set web-browsing-threshold {integer}
  set top-n {integer}
end
```

config report setting

Parameter	Description	Type	Size	Default						
pdf-report	Enable/disable PDF report.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PDF report.</td></tr><tr><td><i>disable</i></td><td>Disable PDF report.</td></tr></table>	Option	Description	<i>enable</i>	Enable PDF report.	<i>disable</i>	Disable PDF report.			
Option	Description									
<i>enable</i>	Enable PDF report.									
<i>disable</i>	Disable PDF report.									
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								
report-source	Report log source.	option	-	forward-traffic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward-traffic</i></td><td>Report includes forward traffic logs.</td></tr><tr><td><i>sniffer-traffic</i></td><td>Report includes sniffer traffic logs.</td></tr><tr><td><i>local-deny-traffic</i></td><td>Report includes local deny traffic logs.</td></tr></table>	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.			
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.											
web-browsing-threshold	Web browsing time calculation threshold (3 - 15 min).	integer	Minimum value: 3 Maximum value: 15	3								
top-n	Number of items to populate (1000 - 20000).	integer	Minimum value: 1000 Maximum value: 20000	1000								

config report sql status

Show report database status.

```
config report sql status
    Description: Show report database status.
end
```

router

This section includes syntax for the following commands:

- [config router policy on page 766](#)
- [config router static on page 768](#)
- [config router static6 on page 770](#)

config router policy

Configure IPv4 routing policies.

```
config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set input-device <name1>, <name2>, ...
    set src <subnet1>, <subnet2>, ...
    set dst <subnet1>, <subnet2>, ...
    set action [deny|permit]
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set start-source-port {integer}
    set end-source-port {integer}
    set gateway {ipv4-address}
    set output-device {string}
    set status [enable|disable]
    set comments {var-string}
    set internet-service-id <id1>, <id2>, ...
    set internet-service-custom <name1>, <name2>, ...
  next
end
```

config router policy

Parameter	Description	Type	Size	Default
seq-num	Sequence number(1-65535).	integer	Minimum value: 1 Maximum value: 2048	0
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
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.									
protocol	Protocol number (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0						
start-port	Start destination port number (1 - 65534).	integer	Minimum value: 0 Maximum value: 65535	1						
end-port	End destination port number (1 - 65534).	integer	Minimum value: 0 Maximum value: 65535	65534						
start-source-port	Start source port number (1 - 65534).	integer	Minimum value: 0 Maximum value: 65535	1						
end-source-port	End source port number (1 - 65534).	integer	Minimum value: 0 Maximum value: 65535	65534						
gateway	IP address of the gateway.	ipv4-address	Not Specified	0.0.0.0						
output-device	Outgoing interface name.	string	Maximum length: 35							
status	Enable/disable this policy route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy route.</td></tr><tr><td><i>disable</i></td><td>Disable this policy route.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.
Option	Description									
<i>enable</i>	Enable this policy route.									
<i>disable</i>	Disable this policy route.									

Parameter	Description	Type	Size	Default
comments	Optional comments.	var-string	Maximum length: 255	
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79	

config router static

Configure IPv4 static routing tables.

```

config router static
  Description: Configure IPv4 static routing tables.
  edit <seq-num>
    set status [enable|disable]
    set dst {ipv4-classnet}
    set src {ipv4-classnet}
    set gateway {ipv4-address}
    set preferred-source {ipv4-address}
    set weight {integer}
    set priority {integer}
    set device {string}
    set comment {var-string}
    set blackhole [enable|disable]
    set sdwan-zone <name1>, <name2>, ...
    set dstaddr {string}
    set link-monitor-exempt [enable|disable]
    set tag {integer}
  next
end

```

config router static

Parameter	Description	Type	Size	Default
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this static route.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable static route.	
	<i>disable</i>		Disable static route.	
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
src	Source prefix for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0
preferred-source	Preferred source IP for this route.	ipv4-address	Not Specified	0.0.0.0
weight	Administrative weight (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0
priority	Administrative priority (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	1
device	Gateway out interface or tunnel.	string	Maximum length: 35	
comment	Optional comments.	var-string	Maximum length: 255	
blackhole	Enable/disable black hole.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable black hole.	
	<i>disable</i>		Disable black hole.	

Parameter	Description	Type	Size	Default						
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79							
dstaddr	Name of firewall address or address group.	string	Maximum length: 79							
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)									
tag	Route tag.	integer	Minimum value: 0 Maximum value: 4294967295	0						

config router static6

Configure IPv6 static routing tables.

```

config router static6
  Description: Configure IPv6 static routing tables.
  edit <seq-num>
    set status [enable|disable]
    set dst {ipv6-network}
    set gateway {ipv6-address}
    set device {string}
    set devindex {integer}
    set weight {integer}
    set priority {integer}
    set comment {var-string}
    set blackhole [enable|disable]
    set sdwan-zone <name1>, <name2>, ...
    set dstaddr {string}
    set link-monitor-exempt [enable|disable]
  next
end

```

config router static6

Parameter	Description	Type	Size	Default
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this static route.	option	-	enable
	Option	Description		
	enable	Enable static route.		
	disable	Disable static route.		
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::
device	Gateway out interface or tunnel.	string	Maximum length: 35	
devindex	Device index (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0
weight	Administrative weight (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0
priority	Administrative priority (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	1024
comment	Optional comments.	var-string	Maximum length: 255	
blackhole	Enable/disable black hole.	option	-	disable
	Option	Description		
	enable	Enable black hole.		
	disable	Disable black hole.		

Parameter	Description	Type	Size	Default
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79	
dstaddr	Name of firewall address or address group.	string	Maximum length: 79	
link- monitor- exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable
		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)	

rule

This section includes syntax for the following commands:

- [config rule fmwP on page 773](#)
- [config rule otdt on page 775](#)
- [config rule otvp on page 777](#)

config rule fmwP

Show FMWP signatures.

```
config rule fmwP
  Description: Show FMWP signatures.
  edit <name>
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set group {string}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set service {user}
    set rule-id {integer}
    set rev {integer}
    set date {integer}
    config metadata
      Description: Meta data.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
  next
end
```

config rule fmwP

Parameter	Description	Type	Size	Default
name	Rule name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
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.		
action	Action.	option	-	pass
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
group	Group.	string	Maximum length: 63	
severity	Severity.	user	Not Specified	
location	Vulnerable location.	user	Not Specified	
os	Vulnerable operation systems.	user	Not Specified	
application	Vulnerable applications.	user	Not Specified	
service	Vulnerable service.	user	Not Specified	
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config rule otdt

Show OT detection signatures.

```
config rule otdt
  Description: Show OT detection signatures.
  edit <name>
    set id {integer}
    set category {integer}
    set popularity {integer}
    set risk {integer}
    set weight {integer}
    set protocol {user}
    set technology {user}
    set behavior {user}
    set vendor {user}
    config parameters
      Description: Application parameters.
      edit <name>
        set default value {string}
      next
    end
  config metadata
    Description: Meta data.
    edit <id>
      set metaid {integer}
      set valueid {integer}
    next
```

```
end
next
end
```

config rule otdt

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

config parameters

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

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config rule otpv

Show OT patch signatures.

```
config rule otpv
  Description: Show OT patch signatures.
  edit <name>
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set group {string}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set service {user}
    set rule-id {integer}
```

```

    set rev {integer}
    set date {integer}
    config metadata
        Description: Meta data.
        edit <id>
            set metaid {integer}
            set valueid {integer}
        next
    end
next
end

```

config rule otvp

Parameter	Description	Type	Size	Default						
name	Rule name.	string	Maximum length: 63							
log	Enable/disable logging.	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.	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.									
action	Action.	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.									
group	Group.	string	Maximum length: 63							
severity	Severity.	user	Not Specified							
location	Vulnerable location.	user	Not Specified							
os	Vulnerable operation systems.	user	Not Specified							
application	Vulnerable applications.	user	Not Specified							

Parameter	Description	Type	Size	Default
service	Vulnerable service.	user	Not Specified	
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 780](#)

config ssh-filter profile

Configure SSH filter profile.

```
config ssh-filter profile
  Description: Configure SSH filter profile.
  edit <name>
    set block {option1}, {option2}, ...
    set log {option1}, {option2}, ...
    set default-command-log [enable|disable]
    config shell-commands
      Description: SSH command filter.
      edit <id>
        set type [simple|regex]
        set pattern {string}
        set action [block|allow]
        set log [enable|disable]
        set alert [enable|disable]
        set severity [low|medium|...]
      next
    end
  next
end
```

config ssh-filter profile

Parameter	Description	Type	Size	Default
name	SSH filter profile name.	string	Maximum length: 35	
block	SSH blocking options.	option	-	
	Option	Description		
	<i>x11</i>	X server forwarding.		
	<i>shell</i>	SSH shell.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
log	SSH logging options.	option	-	
	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
	Option	Description		
	<i>enable</i>	Enable log unmatched shell commands.		
	<i>disable</i>	Disable log unmatched shell commands.		

config shell-commands

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

Parameter	Description	Type	Size	Default
type	Matching type.	option	-	simple
	Option Description			
	<i>simple</i>	Match single command.		
	<i>regex</i>	Match command line using regular expression.		
pattern	SSH shell command pattern.	string	Maximum length: 128	
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.		
log	Enable/disable logging.	option	-	disable
	Option Description			
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
alert	Enable/disable alert.	option	-	disable
	Option Description			
	<i>enable</i>	Enable alert.		
	<i>disable</i>	Disable alert.		
severity	Log severity.	option	-	medium
	Option Description			
	<i>low</i>	Severity low.		
	<i>medium</i>	Severity medium.		
	<i>high</i>	Severity high.		
	<i>critical</i>	Severity critical.		

system

This section includes syntax for the following commands:

- [config system accprofile on page 786](#)
- [config system acme on page 798](#)
- [config system admin on page 799](#)
- [config system affinity-interrupt on page 807](#)
- [config system affinity-packet-redistribution on page 808](#)
- [config system alarm on page 808](#)
- [config system alias on page 812](#)
- [config system api-user on page 812](#)
- [config system arp-table on page 814](#)
- [config system arp on page 814](#)
- [config system auto-install on page 831](#)
- [config system auto-script on page 832](#)
- [config system auto-update status on page 833](#)
- [config system auto-update versions on page 833](#)
- [config system automation-action on page 815](#)
- [config system automation-condition on page 820](#)
- [config system automation-destination on page 822](#)
- [config system automation-stitch on page 822](#)
- [config system automation-trigger on page 824](#)
- [config system autoupdate schedule on page 829](#)
- [config system autoupdate tunneling on page 830](#)
- [config system central-management on page 833](#)
- [config system central-mgmt on page 838](#)
- [config system checksum status on page 839](#)
- [config system cloud-service on page 839](#)
- [config system cmdb on page 840](#)
- [config system console on page 840](#)
- [config system csf on page 841](#)
- [config system custom-language on page 847](#)
- [config system ddns on page 848](#)
- [config system device-upgrade on page 851](#)
- [config system dhcp6 server on page 866](#)
- [config system dhcp server on page 854](#)
- [config system dns-database on page 873](#)
- [config system dns-server on page 876](#)
- [config system dns on page 869](#)

-
- [config system dscp-based-priority on page 877](#)
 - [config system email-server on page 878](#)
 - [config system external-resource on page 880](#)
 - [config system fabric-vpn on page 883](#)
 - [config system federated-upgrade on page 887](#)
 - [config system fips-cc on page 891](#)
 - [config system fortianalyzer-connectivity on page 892](#)
 - [config system fortiguard-log-service on page 903](#)
 - [config system fortiguard-service on page 903](#)
 - [config system fortiguard on page 892](#)
 - [config system fortindr on page 903](#)
 - [config system fortisandbox on page 904](#)
 - [config system fsso-polling on page 906](#)
 - [config system ftm-push on page 907](#)
 - [config system geoip-country on page 908](#)
 - [config system geoip-override on page 908](#)
 - [config system global on page 910](#)
 - [config system gre-tunnel on page 956](#)
 - [config system ha-lic on page 970](#)
 - [config system ha-monitor on page 970](#)
 - [config system ha-nonsync-csum on page 971](#)
 - [config system ha on page 958](#)
 - [config system info admin ssh on page 971](#)
 - [config system info admin status on page 972](#)
 - [config system interface on page 972](#)
 - [config system ip-conflict status on page 1015](#)
 - [config system ipam on page 1008](#)
 - [config system ips-urlfilter-dns on page 1013](#)
 - [config system ips-urlfilter-dns6 on page 1013](#)
 - [config system ips on page 1012](#)
 - [config system ipv6-neighbor-cache on page 1014](#)
 - [config system link-monitor on page 1015](#)
 - [config system management-tunnel on page 1020](#)
 - [config system mgmt-csum on page 1022](#)
 - [config system nethsm on page 1022](#)
 - [config system network-visibility on page 1026](#)
 - [config system ntp on page 1027](#)
 - [config system object-tagging on page 1030](#)
 - [config system password-policy-guest-admin on page 1034](#)
 - [config system password-policy on page 1032](#)
 - [config system performance status on page 1036](#)
 - [config system performance top on page 1037](#)
 - [config system probe-response on page 1037](#)

-
- [config system proxy-arp on page 1039](#)
 - [config system ptp on page 1039](#)
 - [config system replacemsg-group on page 1057](#)
 - [config system replacemsg-image on page 1070](#)
 - [config system replacemsg admin on page 1041](#)
 - [config system replacemsg alertmail on page 1042](#)
 - [config system replacemsg auth on page 1043](#)
 - [config system replacemsg automation on page 1044](#)
 - [config system replacemsg custom-message on page 1045](#)
 - [config system replacemsg fortiguard-wf on page 1046](#)
 - [config system replacemsg ftp on page 1047](#)
 - [config system replacemsg http on page 1048](#)
 - [config system replacemsg icap on page 1049](#)
 - [config system replacemsg mail on page 1050](#)
 - [config system replacemsg nac-quar on page 1051](#)
 - [config system replacemsg spam on page 1052](#)
 - [config system replacemsg sslvpn on page 1053](#)
 - [config system replacemsg traffic-quota on page 1054](#)
 - [config system replacemsg utm on page 1055](#)
 - [config system replacemsg webproxy on page 1056](#)
 - [config system resource-limits on page 1071](#)
 - [config system saml on page 1073](#)
 - [config system sdn-connector on page 1077](#)
 - [config system sdn-proxy on page 1086](#)
 - [config system session-ttl on page 1087](#)
 - [config system session on page 1087](#)
 - [config system session6 on page 1087](#)
 - [config system settings on page 1088](#)
 - [config system sms-server on page 1104](#)
 - [config system snmp community on page 1104](#)
 - [config system snmp mib-view on page 1112](#)
 - [config system snmp sysinfo on page 1112](#)
 - [config system snmp user on page 1114](#)
 - [config system source-ip status on page 1120](#)
 - [config system span-port on page 1120](#)
 - [config system speed-test-schedule on page 1121](#)
 - [config system speed-test-server on page 1124](#)
 - [config system speed-test-setting on page 1125](#)
 - [config system ssh-config on page 1126](#)
 - [config system sso-admin on page 1130](#)
 - [config system sso-forticloud-admin on page 1131](#)
 - [config system sso-fortigate-cloud-admin on page 1131](#)
 - [config system startup-error-log on page 1132](#)

- [config system status on page 1132](#)
- [config system storage on page 1132](#)
- [config system timezone on page 1134](#)
- [config system vdom-dns on page 1135](#)
- [config system vdom-exception on page 1137](#)
- [config system vdom-link on page 1140](#)
- [config system vdom-property on page 1140](#)
- [config system vdom-radius-server on page 1142](#)
- [config system vdom on page 1134](#)
- [config system vne-tunnel on page 1142](#)
- [config system vxlan on page 1144](#)
- [config system wccp on page 1145](#)
- [config system zone on page 1149](#)

config system accprofile

Configure access profiles for system administrators.

```
config system accprofile
  Description: Configure access profiles for system administrators.
  edit <name>
    set scope [vdom|global]
    set comments {var-string}
    set secfabgrp [none|read|...]
    set ftviewgrp [none|read|...]
    set authgrp [none|read|...]
    set sysgrp [none|read|...]
    set netgrp [none|read|...]
    set loggrp [none|read|...]
    set fwgrp [none|read|...]
    set vpngrp [none|read|...]
    set utmgrp [none|read|...]
    set wanoptgrp [none|read|...]
    config netgrp-permission
      Description: Custom network permission.
      set cfg [none|read|...]
      set packet-capture [none|read|...]
      set route-cfg [none|read|...]
    end
    config sysgrp-permission
      Description: Custom system permission.
      set admin [none|read|...]
      set upd [none|read|...]
      set cfg [none|read|...]
      set mnt [none|read|...]
    end
    config fwgrp-permission
      Description: Custom firewall permission.
```

```

        set policy [none|read|...]
        set address [none|read|...]
        set service [none|read|...]
        set schedule [none|read|...]
        set others [none|read|...]
    end
    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
    config utmgrp-permission
        Description: Custom Security Profile permissions.
        set antivirus [none|read|...]
        set ips [none|read|...]
        set webfilter [none|read|...]
        set emailfilter [none|read|...]
        set dlp [none|read|...]
        set file-filter [none|read|...]
        set application-control [none|read|...]
        set icap [none|read|...]
        set voip [none|read|...]
        set waf [none|read|...]
        set dnsfilter [none|read|...]
        set endpoint-control [none|read|...]
        set videofilter [none|read|...]
        set virtual-patch [none|read|...]
        set casb [none|read|...]
    end
    set admintimeout-override [enable|disable]
    set admintimeout {integer}
    set cli-diagnose [enable|disable]
    set cli-get [enable|disable]
    set cli-show [enable|disable]
    set cli-exec [enable|disable]
    set cli-config [enable|disable]
    set system-execute-ssh [enable|disable]
    set system-execute-telnet [enable|disable]
next
end

```

config system accprofile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default										
scope	Scope of admin access: global or specific VDOM(s).	option	-	vdom										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vdom</i></td><td>VDOM access.</td></tr><tr><td><i>global</i></td><td>Global access.</td></tr></table>	Option	Description	<i>vdom</i>	VDOM access.	<i>global</i>	Global access.							
Option	Description													
<i>vdom</i>	VDOM access.													
<i>global</i>	Global access.													
comments	Comment.	var-string	Maximum length: 255											
secfabgrp	Security Fabric.	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.													
ftviewgrp	FortiView.	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.													
authgrp	Administrator access to Users and Devices.	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.													
sysgrp	System Configuration.	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><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
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										
netgrp	Network Configuration.	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><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
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										
	<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><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
fwgrp	Administrator access to the Firewall configuration.	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><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	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><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.													
utmgrp	Administrator access to Security Profiles.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr></table>	Option	Description	<i>none</i>	No access.									
Option	Description													
<i>none</i>	No access.													

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></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><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
	Option	Description										
	<i>read</i>	Read access.										
	<i>read-write</i>	Read/write access.										
<i>custom</i>	Customized access.											
wanoptgrp	Administrator access to WAN Opt & Cache.	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.											
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overriding the global administrator idle timeout.</td></tr><tr><td><i>disable</i></td><td>Disable overriding the global administrator idle timeout.</td></tr></table>	Option	Description	<i>enable</i>	Enable overriding the global administrator idle timeout.	<i>disable</i>	Disable overriding the global administrator idle timeout.					
	Option	Description										
	<i>enable</i>	Enable overriding the global administrator idle timeout.										
<i>disable</i>	Disable overriding the global administrator idle timeout.											
admintimeout	Administrator timeout for this access profile (0 - 480 min, default = 10, 0 means never timeout).	integer	Minimum value: 1 Maximum value: 480	10								
cli-diagnose	Enable/disable permission to run diagnostic commands.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable permission to run diagnostic commands.</td></tr><tr><td><i>disable</i></td><td>Disable permission to run diagnostic commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable permission to run diagnostic commands.	<i>disable</i>	Disable permission to run diagnostic commands.					
	Option	Description										
	<i>enable</i>	Enable permission to run diagnostic commands.										
<i>disable</i>	Disable permission to run diagnostic commands.											
cli-get	Enable/disable permission to run get commands.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable permission to run get commands.</td></tr><tr><td><i>disable</i></td><td>Disable permission to run get commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable permission to run get commands.	<i>disable</i>	Disable permission to run get commands.					
	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								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable permission to run show commands.		
	<i>disable</i>	Disable permission to run show commands.		
cli-exec	Enable/disable permission to run execute commands.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable permission to run execute commands.		
	<i>disable</i>	Disable permission to run execute commands.		
cli-config	Enable/disable permission to run config commands.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable permission to run config commands.		
	<i>disable</i>	Disable permission to run config commands.		
system-execute-ssh	Enable/disable permission to execute SSH commands.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable permission to execute SSH commands.		
	<i>disable</i>	Disable permission to execute SSH commands.		
system-execute-telnet	Enable/disable permission to execute TELNET commands.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable permission to execute TELNET commands.		
	<i>disable</i>	Disable permission to execute TELNET commands.		

config netgrp-permission

Parameter	Description	Type	Size	Default
cfg	Network Configuration.	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.		
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.		
upd	FortiGuard Updates.	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
mnt	Maintenance.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config fwgrp-permission

Parameter	Description	Type	Size	Default
policy	Policy Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
address	Address Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
service	Service 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

Parameter	Description	Type	Size	Default
	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.		

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config utmgrp-permission

Parameter	Description	Type	Size	Default
antivirus	Antivirus 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.		
webfilter	Web 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.		
dlp	DLP profiles 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.		
file-filter	File-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.		
application-control	Application Control profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<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.		
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.		
waf	Web Application Firewall 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.		
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.		
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.		
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.		
casb	Inline CASB filter profile and settings	option	-	none
	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.
  set interface <interface-name1>, <interface-name2>, ...
  set use-ha-direct [enable|disable]
  set source-ip {ipv4-address}
  set source-ip6 {ipv6-address}
  config accounts
    Description: ACME accounts list.
    edit <id>
      set status {string}
      set url {string}
      set ca_url {string}
      set email {string}
      set privatekey {string}
    next
  end
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							
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						
	<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-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	::						

config accounts

Parameter	Description	Type	Size	Default
id	Account id.	string	Maximum length: 255	
status	Account status.	string	Maximum length: 127	
url	Account url.	string	Maximum length: 511	
ca_url	Account ca_url.	string	Maximum length: 255	
email	Account email.	string	Maximum length: 255	
privatekey	Account Private Key.	string	Maximum length: 8191	

config system admin

Configure admin users.

```
config system admin
  Description: Configure admin users.
  edit <name>
    set wildcard [enable|disable]
    set remote-auth [enable|disable]
    set remote-group {string}
    set password {password-2}
    set peer-auth [enable|disable]
    set peer-group {string}
    set trusthost1 {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 trusthost10 {ipv4-classnet}
    set ip6-trusthost1 {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 ip6-trusthost10 {ipv6-prefix}
set accprofile {string}
set allow-remove-admin-session [enable|disable]
set comments {var-string}
set vdom <name1>, <name2>, ...
set ssh-public-key1 {user}
set ssh-public-key2 {user}
set ssh-public-key3 {user}
set ssh-certificate {string}
set schedule {string}
set accprofile-override [enable|disable]
set vdom-override [enable|disable]
set password-expire {user}
set force-password-change [enable|disable]
set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set fortitoken {string}
set email-to {string}
set sms-server [fortiguard|custom]
set sms-custom-server {string}
set sms-phone {string}
set guest-auth [disable|enable]
set guest-usergroups <name1>, <name2>, ...
set guest-lang {string}
config trusthosts
    Description: Table of trusthosts.
    edit <id>
        set type [ipv4|ipv6]
        set ipv4 {ipv4-classnet}
        set ipv6 {ipv6-prefix}
    next
end
next
end

```

config system admin

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 64	
wildcard	Enable/disable wildcard RADIUS 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 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.									
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							
password	Admin user password.	password-2	Not Specified							
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							
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiProxy 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 FortiProxy 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 FortiProxy 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 FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0

Parameter	Description	Type	Size	Default
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiProxy features.	string	Maximum length: 35	
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable
	Option	Description		
	enable	Enable allow-remove option.		
	disable	Disable allow-remove option.		
comments	Comment.	var-string	Maximum length: 255	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	
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	
ssh-certificate	Select the certificate to be used by the FortiProxy for authentication with an SSH client.	string	Maximum length: 35	
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35	
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiProxy features that this administrator can access.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable access profile override.		
	<i>disable</i>	Disable access profile override.		
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
	Option	Description		
	<i>enable</i>	Enable VDOM override.		
	<i>disable</i>	Disable VDOM override.		
password-expire	Password expire time.	user	Not Specified	
force-password-change	Enable/disable force password change on next login.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable force password change on next login.		
	<i>disable</i>	Disable force password change on next login.		
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable two-factor authentication.		
	<i>fortitoken</i>	Use FortiToken or FortiToken mobile two-factor authentication.		
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.		
	<i>email</i>	Send a two-factor authentication code to the configured email-to email address.		
	<i>sms</i>	Send a two-factor authentication code to the configured sms-server and sms-phone.		
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	

Parameter	Description	Type	Size	Default								
	<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.											
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16									
email-to	This administrator's email address.	string	Maximum length: 63									
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><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.					
	Option	Description										
	<i>fortiguard</i>	Send SMS by FortiGuard.										
<i>custom</i>	Send SMS by custom server.											
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									
guest-auth	Enable/disable guest authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable guest authentication.</td></tr><tr><td><i>enable</i></td><td>Enable guest authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable guest authentication.	<i>enable</i>	Enable guest authentication.					
	Option	Description										
	<i>disable</i>	Disable guest authentication.										
<i>enable</i>	Enable guest authentication.											
guest-usergroups <name>	Select guest user groups. Select guest user groups.	string	Maximum length: 79									
guest-lang	Guest management portal language.	string	Maximum length: 35									

config trusthosts

Parameter	Description	Type	Size	Default						
type	Trusthost type.	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 trusthost.</td></tr><tr><td>ipv6</td><td>IPv6 trusthost.</td></tr></table>	Option	Description	ipv4	IPv4 trusthost.	ipv6	IPv6 trusthost.			
	Option	Description								
	ipv4	IPv4 trusthost.								
ipv6	IPv6 trusthost.									
ipv4	IPv4 trusthost.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
ipv6	IPv6 trusthost.	ipv6-prefix	Not Specified	::/0						

config system affinity-interrupt

Configure interrupt affinity.

```
config system affinity-interrupt
  Description: Configure interrupt affinity.
  edit <id>
    set interrupt {string}
    set affinity-cpumask {string}
    set default-affinity-cpumask {string}
  next
end
```

config system affinity-interrupt

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	
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).	string	Maximum length: 127	

config system affinity-packet-redistribution

Configure packet redistribution.

```
config system affinity-packet-redistribution
  Description: Configure packet redistribution.
  edit <id>
    set interface {string}
    set rxqid {integer}
    set round-robin [enable|disable]
    set affinity-cpumask {string}
  next
end
```

config system affinity-packet-redistribution

Parameter	Description	Type	Size	Default						
id	ID of the packet redistribution setting.	integer	Minimum value: 0 Maximum value: 4294967295	0						
interface	Physical interface name on which to perform packet redistribution.	string	Maximum length: 15							
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						
round-robin	Enable/disable round-robin redistribution to multiple CPUs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable round-robin redistribution.</td></tr><tr><td><i>disable</i></td><td>Disable round-robin redistribution.</td></tr></table>				Option	Description	<i>enable</i>	Enable round-robin redistribution.	<i>disable</i>	Disable round-robin redistribution.
	Option	Description								
	<i>enable</i>	Enable round-robin redistribution.								
<i>disable</i>	Disable round-robin redistribution.									
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127							

config system alarm

Configure alarm.

```

config system alarm
    Description: Configure alarm.
    set status [enable|disable]
    set audible [enable|disable]
    config groups
        Description: Alarm groups.
        edit <id>
            set period {integer}
            set admin-auth-failure-threshold {integer}
            set admin-auth-lockout-threshold {integer}
            set user-auth-failure-threshold {integer}
            set user-auth-lockout-threshold {integer}
            set replay-attempt-threshold {integer}
            set self-test-failure-threshold {integer}
            set log-full-warning-threshold {integer}
            set encryption-failure-threshold {integer}
            set decryption-failure-threshold {integer}
            config fw-policy-violations
                Description: Firewall policy violations.
                edit <id>
                    set threshold {integer}
                    set src-ip {ipv4-address}
                    set dst-ip {ipv4-address}
                    set src-port {integer}
                    set dst-port {integer}
                next
            end
            set fw-policy-id {integer}
            set fw-policy-id-threshold {integer}
        next
    end
end

```

config system alarm

Parameter	Description	Type	Size	Default						
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.									
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.									

config groups

Parameter	Description	Type	Size	Default
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	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
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
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024	0

Parameter	Description	Type	Size	Default
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
decryption-failure-threshold	Decryption 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

config fw-policy-violations

Parameter	Description	Type	Size	Default
id	Firewall policy violations ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024	0
src-ip	Source IP (0=all).	ipv4-address	Not Specified	0.0.0.0
dst-ip	Destination 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
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535	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
name	Alias command name.	string	Maximum length: 35	
command	Command list to execute.	var-string	Maximum length: 255	

config system api-user

Configure API users.

```
config system api-user
  Description: Configure API users.
  edit <name>
    set comments {var-string}
    set api-key {password-2}
    set accprofile {string}
    set vdom <name1>, <name2>, ...
    set schedule {string}
    set cors-allow-origin {string}
    set peer-auth [enable|disable]
    set peer-group {string}
    config trusthost
      Description: Trusthost.
      edit <id>
        set type [ipv4-trusthost|ipv6-trusthost]
        set ipv4-trusthost {ipv4-classnet}
        set ipv6-trusthost {ipv6-prefix}
      next
    end
  next
end
```


config system api-user

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 255	
api-key	Admin user password.	password-2	Not Specified	
accprofile	Admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79	
schedule	Schedule name.	string	Maximum length: 35	
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible.	string	Maximum length: 269	
peer-auth	Enable/disable peer authentication.	option	-	disable
	Option	Description		
	enable	Enable peer.		
	disable	Disable peer.		
peer-group	Peer group name.	string	Maximum length: 35	

config trusthost

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Trusthost type.	option	-	ipv4-trusthost
	Option	Description		
	ipv4-trusthost	IPv4 trusthost.		
	ipv6-trusthost	IPv6 trusthost.		

Parameter	Description	Type	Size	Default
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

config system arp

IPv4 ARP table.

```
config system arp
    Description: IPv4 ARP table.
end
```

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 description {var-string}
    set action-type [email|fortiexplorer-notification|...]
    set system-action [reboot|shutdown|...]
    set tls-certificate {string}
    set forticare-email [enable|disable]
    set email-to <name1>, <name2>, ...
    set email-from {var-string}
    set email-subject {var-string}
    set minimum-interval {integer}
    set aws-api-key {password}
    set azure-function-authorization [anonymous|function|...]
    set azure-api-key {password}
    set alicloud-function-authorization [anonymous|function]
    set alicloud-access-key-id {string}
    set alicloud-access-key-secret {password}
    set message-type [text|json]
    set message {string}
    set replacement-message [enable|disable]
    set replacemsg-group {string}
    set protocol [http|https]
    set method [post|put|...]
    set uri {var-string}
    set http-body {var-string}
    set port {integer}
    config http-headers
      Description: Request headers.
      edit <id>
        set key {var-string}
        set value {var-string}
      next
    end
    set verify-host-cert [enable|disable]
    set script {var-string}
    set output-size {integer}
    set timeout {integer}
    set password {password}
    set execute-security-fabric [enable|disable]
    set accprofile {string}
    set security-tag {string}
    set sdn-connector <name1>, <name2>, ...
  next
end
```

config system automation-action

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 64	
description	Description.	var-string	Maximum length: 255	
action-type	Action type.	option	-	alert
	Option	Description		
	<i>email</i>	Send notification email.		
	<i>fortiexplorer-notification</i>	Send push notification to FortiExplorer.		
	<i>alert</i>	Generate FortiProxy dashboard alert.		
	<i>disable-ssid</i>	Disable interface.		
	<i>system-actions</i>	Perform immediate system operations on this FortiGate unit.		
	<i>quarantine</i>	Quarantine host.		
	<i>quarantine-forticlient</i>	Quarantine FortiClient by EMS.		
	<i>quarantine-nsx</i>	Quarantine NSX instance.		
	<i>quarantine-fortinac</i>	Quarantine host by FortiNAC.		
	<i>ban-ip</i>	Ban IP address.		
	<i>aws-lambda</i>	Send log data to integrated AWS service.		
	<i>azure-function</i>	Send log data to an Azure function.		
	<i>google-cloud-function</i>	Send log data to a Google Cloud function.		
	<i>alicloud-function</i>	Send log data to an AliCloud function.		
	<i>webhook</i>	Send an HTTP request.		
	<i>cli-script</i>	Run CLI script.		
	<i>slack-notification</i>	Send a notification message to a Slack incoming webhook.		
	<i>microsoft-teams-notification</i>	Send a notification message to a Microsoft Teams incoming webhook.		

Parameter	Description	Type	Size	Default								
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.											
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35									
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.											
email-to <name>	Email addresses. Email address.	string	Maximum length: 255									
email-from	Email sender name.	var-string	Maximum length: 127									
email-subject	Email subject.	var-string	Maximum length: 511									
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0								
aws-api-key	AWS API Gateway API key.	password	Not Specified									
azure-function-authorization	Azure function authorization level.	option	-	anonymous								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization level (No authorization required).</td></tr></table>	Option	Description	<i>anonymous</i>	Anonymous authorization level (No authorization required).							
	Option	Description										
<i>anonymous</i>	Anonymous authorization level (No authorization required).											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></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>function</i>	Function authorization level (Function or Host Key required).	<i>admin</i>	Admin authorization level (Master Host Key required).			
	Option	Description								
	<i>function</i>	Function authorization level (Function or Host Key required).								
<i>admin</i>	Admin authorization level (Master Host Key required).									
azure-api-key	Azure function API key.	password	Not Specified							
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization (Authorization required).</td></tr></table>	Option	Description	<i>anonymous</i>	Anonymous authorization (No authorization required).	<i>function</i>	Function authorization (Authorization required).			
	Option	Description								
	<i>anonymous</i>	Anonymous authorization (No authorization required).								
<i>function</i>	Function authorization (Authorization required).									
alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35							
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified							
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.									
message	Message content.	string	Maximum length: 4095	%%log%%						
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							
protocol	Request protocol.	option	-	http						

Parameter	Description	Type	Size	Default												
	<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.															
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.															
uri	Request API URI.	var-string	Maximum length: 1023													
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 4095													
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0												
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.															
script	CLI script.	var-string	Maximum length: 1023													
output-size	Number of megabytes to limit script output to (1 - 1024, default = 10).	integer	Minimum value: 1 Maximum value: 1024	10												

Parameter	Description	Type	Size	Default						
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0						
password	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for sftp/ftp server password.	password	Not Specified							
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.									
accprofile	Access profile for CLI script action to access FortiProxy features.	string	Maximum length: 35							
security-tag	NSX security tag.	string	Maximum length: 255							
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79							

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 description {var-string}
        set condition-type [cpu|memory|...]
        set cpu-usage-percent {integer}
        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								
name	Name.	string	Maximum length: 35									
description	Description.	var-string	Maximum length: 255									
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 Maximum value: 100	0								
mem-usage-percent	Memory usage reaches specified percentage.	integer	Minimum value: 0 Maximum value: 100	0								
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								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tunnel-up</i>	VPN tunnel is up.		
	<i>tunnel-down</i>	VPN tunnel is down.		

config system automation-destination

Automation destinations.

```
config system automation-destination
  Description: Automation destinations.
  edit <name>
    set type [fortiproxy|ha-cluster]
    set destination <name1>, <name2>, ...
    set ha-group-id {integer}
  next
end
```

config system automation-destination

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Destination type.	option	-	fortiproxy
	Option	Description		
	<i>fortiproxy</i>	FortiProxy set as destination.		
	<i>ha-cluster</i>	HA cluster set as destination.		
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

config system automation-stitch

Automation stitches.

```

config system automation-stitch
    Description: Automation stitches.
    edit <name>
        set description {var-string}
        set status [enable|disable]
        set trigger {string}
        set condition <name1>, <name2>, ...
        set condition-logic [and|or]
    config actions
        Description: Configure stitch actions.
        edit <id>
            set action {string}
            set delay {integer}
            set required [enable|disable]
        next
    end
    set destination <name1>, <name2>, ...
next
end

```

config system automation-stitch

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
description	Description.	var-string	Maximum length: 255	
status	Enable/disable this stitch.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable stitch.		
	<i>disable</i>	Disable stitch.		
trigger	Trigger name.	string	Maximum length: 35	
condition <name>	Automation conditions. Condition name.	string	Maximum length: 79	
condition-logic	Apply AND/OR logic to the specified automation conditions.	option	-	and
	Option	Description		
	<i>and</i>	All specified conditions must be met.		
	<i>or</i>	At least one specified condition needs to be met.		

Parameter	Description	Type	Size	Default
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79	

config actions

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Action name.	string	Maximum length: 64	
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	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 trigger-type [event-based|scheduled]
    set event-type [ioc|event-log|...]
    set vdom <name1>, <name2>, ...
    set license-type [forticare-support|fortiguard-webfilter|...]
    set report-type [posture|coverage|...]
    set logid <id1>, <id2>, ...
    set trigger-frequency [hourly|daily|...]
    set trigger-weekday [sunday|monday|...]
    set trigger-day {integer}
    set trigger-hour {integer}
  
```

```

set trigger-minute {integer}
set trigger-datetime {datetime}
config fields
    Description: Customized trigger field settings.
    edit <id>
        set name {string}
        set value {var-string}
    next
end
set faz-event-name {var-string}
set faz-event-severity {var-string}
set faz-event-tags {var-string}
set serial {var-string}
set fabric-event-name {var-string}
set fabric-event-severity {var-string}
next
end

```

config system automation-trigger

Parameter	Description	Type	Size	Default												
name	Name.	string	Maximum length: 35													
description	Description.	var-string	Maximum length: 255													
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.															
event-type	Event type.	option	-	ioc												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ioc</i></td><td>Indicator of compromise detected.</td></tr><tr><td><i>event-log</i></td><td>Use log ID as trigger.</td></tr><tr><td><i>reboot</i></td><td>Device reboot.</td></tr><tr><td><i>low-memory</i></td><td>Conserve mode due to low memory.</td></tr><tr><td><i>high-cpu</i></td><td>High CPU usage.</td></tr></table>				Option	Description	<i>ioc</i>	Indicator of compromise detected.	<i>event-log</i>	Use log ID as trigger.	<i>reboot</i>	Device reboot.	<i>low-memory</i>	Conserve mode due to low memory.	<i>high-cpu</i>	High CPU usage.
	Option	Description														
	<i>ioc</i>	Indicator of compromise detected.														
	<i>event-log</i>	Use log ID as trigger.														
	<i>reboot</i>	Device reboot.														
	<i>low-memory</i>	Conserve mode due to low memory.														
<i>high-cpu</i>	High CPU usage.															

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>license-near-expiry</i></td><td>License near expiration date.</td></tr><tr><td><i>local-cert-near-expiry</i></td><td>The local certificate near expiration date.</td></tr><tr><td><i>ha-failover</i></td><td>HA failover.</td></tr><tr><td><i>config-change</i></td><td>Configuration change.</td></tr><tr><td><i>security-rating-summary</i></td><td>Security rating summary.</td></tr><tr><td><i>virus-ips-db-updated</i></td><td>Virus and IPS database updated.</td></tr><tr><td><i>faz-event</i></td><td>FortiAnalyzer event.</td></tr><tr><td><i>incoming-webhook</i></td><td>Incoming webhook call.</td></tr><tr><td><i>fabric-event</i></td><td>Fabric connector event.</td></tr><tr><td><i>ips-logs</i></td><td>IPS logs.</td></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></table>	Option	Description	<i>license-near-expiry</i>	License near expiration date.	<i>local-cert-near-expiry</i>	The local certificate near expiration date.	<i>ha-failover</i>	HA failover.	<i>config-change</i>	Configuration change.	<i>security-rating-summary</i>	Security rating summary.	<i>virus-ips-db-updated</i>	Virus and IPS database updated.	<i>faz-event</i>	FortiAnalyzer event.	<i>incoming-webhook</i>	Incoming webhook call.	<i>fabric-event</i>	Fabric connector event.	<i>ips-logs</i>	IPS logs.	<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.			
	Option	Description																																		
	<i>license-near-expiry</i>	License near expiration date.																																		
	<i>local-cert-near-expiry</i>	The local certificate near expiration date.																																		
	<i>ha-failover</i>	HA failover.																																		
	<i>config-change</i>	Configuration change.																																		
	<i>security-rating-summary</i>	Security rating summary.																																		
	<i>virus-ips-db-updated</i>	Virus and IPS database updated.																																		
	<i>faz-event</i>	FortiAnalyzer event.																																		
	<i>incoming-webhook</i>	Incoming webhook call.																																		
	<i>fabric-event</i>	Fabric connector event.																																		
	<i>ips-logs</i>	IPS logs.																																		
	<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.																																			
vdom <name>	Virtual domain(s) that this trigger is valid for. Virtual domain name.	string	Maximum length: 79																																	
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></table>	Option	Description	<i>forticare-support</i>	FortiCare support license.																															
	Option	Description																																		
<i>forticare-support</i>	FortiCare support license.																																			

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></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>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>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.																			
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.																			
logid <id>	Log IDs to trigger event. Log ID.	integer	Minimum value: 1 Maximum value: 65535																	
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-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.																			
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31	1																
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-datetime	Trigger date and time (YYYY-MM-DD HH:MM:SS).	datetime	Not Specified	0000-00-00 00:00:00																
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																	
serial	Fabric connector serial number.	var-string	Maximum length: 255																	
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																	

config fields

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

config system autoupdate schedule

Configure update schedule.

```
config system autoupdate schedule
  Description: Configure update schedule.
  set status [enable|disable]
  set frequency [every|daily|...]
  set time {user}
  set day [Sunday|Monday|...]
end
```

config system autoupdate schedule

Parameter	Description	Type	Size	Default								
status	Enable/disable scheduled updates.	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.											
frequency	Update frequency.	option	-	automatic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>every</i></td><td>Time interval.</td></tr><tr><td><i>daily</i></td><td>Every day.</td></tr><tr><td><i>weekly</i></td><td>Every week.</td></tr></table>	Option	Description	<i>every</i>	Time interval.	<i>daily</i>	Every day.	<i>weekly</i>	Every week.			
Option	Description											
<i>every</i>	Time interval.											
<i>daily</i>	Every day.											
<i>weekly</i>	Every week.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>automatic</i>	Update automatically within every one hour period.		
time	Update time.	user	Not Specified	
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.		

config system autoupdate tunneling

Configure web proxy tunneling for the FDN.

```
config system autoupdate tunneling
  Description: Configure web proxy tunneling for the FDN.
  set status [enable|disable]
  set address {string}
  set port {integer}
  set username {string}
  set password {password}
end
```

config system autoupdate tunneling

Parameter	Description	Type	Size	Default
status	Enable/disable web proxy tunneling.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
address	Web proxy IP address or FQDN.	string	Maximum length: 63	
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535	0
username	Web proxy username.	string	Maximum length: 49	
password	Web proxy password.	password	Not Specified	

config system auto-install

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.									
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.									

Parameter	Description	Type	Size	Default
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fpx_system.conf
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out

config system auto-script

Configure auto script.

```

config system auto-script
  Description: Configure auto script.
  edit <name>
    set interval {integer}
    set repeat {integer}
    set start [manual|auto]
    set script {var-string}
    set password {password}
    set output-size {integer}
    set timeout {integer}
  next
end

```

config system auto-script

Parameter	Description	Type	Size	Default
name	Auto script name.	string	Maximum length: 35	
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1
start	Script starting mode.	option	-	manual

Parameter	Description	Type	Size	Default						
	<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.									
script	List of FortiProxy CLI commands to repeat.	var-string	Maximum length: 1023							
password	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for sftp/ftp server password.	password	Not Specified							
output-size	Number of megabytes to limit script output to (10 - 1024, default = 10).	integer	Minimum value: 10 Maximum value: 1024	10						
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0						

config system auto-update status

Status of automatic updates.

```
config system auto-update status
    Description: Status of automatic updates.
end
```

config system auto-update versions

Update object versions.

```
config system auto-update versions
    Description: Update object versions.
end
```

config system central-management

Configure central management.

```

config system central-management
    Description: Configure central management.
    set mode [normal|backup]
    set type [fortimanager|fortiguard|...]
    set fortigate-cloud-sso-default-profile {string}
    set schedule-config-restore [enable|disable]
    set schedule-script-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set allow-remote-firmware-upgrade [enable|disable]
    set allow-monitor [enable|disable]
    set serial-number {user}
    set fmg {user}
    set fmg-source-ip {ipv4-address}
    set fmg-source-ip6 {ipv6-address}
    set local-cert {string}
    set ca-cert {user}
    set vdom {string}
    config server-list
        Description: Additional servers that the FortiProxy can use for updates (for AV, IPS,
updates) and ratings (for web filter and antispam ratings) servers.
        edit <id>
            set server-type {option1}, {option2}, ...
            set addr-type [ipv4|ipv6|...]
            set server-address {ipv4-address}
            set server-address6 {ipv6-address}
            set fqdn {string}
        next
    end
    set fmg-update-port [8890|443]
    set include-default-servers [enable|disable]
    set enc-algorithm [default|high|...]
    set interface-select-method [auto|specify]
    set interface {string}
end

```

config system central-management

Parameter	Description	Type	Size	Default
mode	Central management mode.	option	-	normal
type	Option	Description		
	<i>normal</i>	Manage and configure this FortiProxy from FortiManager.		
	<i>backup</i>	Manage and configure this FortiProxy locally and back up its configuration to FortiManager.		
type	Central management type.	option	-	none

Parameter	Description	Type	Size	Default
	Option Description			
	<i>fortimanager</i>	FortiManager.		
	<i>fortiguard</i>	Central management of this FortiProxy using FortiCloud.		
	<i>none</i>	No central management.		
fortigate-cloud-sso-default-profile	Override access profile.	string	Maximum length: 35	
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiProxy.	option	-	enable
	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 FortiProxy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable scheduled script restore.		
	<i>disable</i>	Disable scheduled script restore.		
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiProxy.	option	-	enable
	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 FortiProxy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		

Parameter	Description	Type	Size	Default						
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiProxy 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-monitor	Enable/disable allowing the central management server to remotely monitor this FortiProxy 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.									
serial-number	Serial number.	user	Not Specified							
fmg	IP address or FQDN of the FortiManager.	user	Not Specified							
fmg-source-ip	IPv4 source address that this FortiProxy uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0						
fmg-source-ip6	IPv6 source address that this FortiProxy uses when communicating with FortiManager.	ipv6-address	Not Specified	::						
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35							
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified							
vdom	Virtual domain (VDOM) name to use when communicating with FortiManager.	string	Maximum length: 31	root						
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><i>8890</i></td><td>Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr></table>	Option	Description	<i>8890</i>	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.					
Option	Description									
<i>8890</i>	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></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	443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.							
Option	Description											
443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.											
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.											
enc-algorithm	Encryption strength for communications between the FortiProxy and central management.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>High strength algorithms and medium-strength 128-bit key length algorithms.</td></tr><tr><td>high</td><td>128-bit and larger key length algorithms.</td></tr><tr><td>low</td><td>64-bit or 56-bit key length algorithms without export restrictions.</td></tr></table>	Option	Description	default	High strength algorithms and medium-strength 128-bit key length algorithms.	high	128-bit and larger key length algorithms.	low	64-bit or 56-bit key length algorithms without export restrictions.			
Option	Description											
default	High strength algorithms and medium-strength 128-bit key length algorithms.											
high	128-bit and larger key length algorithms.											
low	64-bit or 56-bit key length algorithms without export restrictions.											
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>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.					
Option	Description											
auto	Set outgoing interface automatically.											
specify	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

config server-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-type	FortiGuard service type.	option	-	
	Option Description			
	<i>update</i>	AV, IPS, and AV-query update server.		
	<i>rating</i>	Web filter and anti-spam rating server.		
	<i>iot-query</i>	IoT query server.		
	<i>iot-collect</i>	IoT device collection server.		
addr-type	Indicate whether the FortiProxy communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4
	Option Description			
	<i>ipv4</i>	IPv4 address.		
	<i>ipv6</i>	IPv6 address.		
	<i>fqdn</i>	FQDN.		
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	::
fqdn	FQDN address of override server.	string	Maximum length: 255	

config system central-mgmt

Configuration of Central Management Service.

```
config system central-mgmt
    Description: Configuration of Central Management Service.
end
```

config system checksum status

System checksum.

```
config system checksum status
    Description: System checksum.
end
```

config system cloud-service

Configure system cloud service.

```
config system cloud-service
    Description: Configure system cloud service.
    edit <name>
        set vendor [unknown|google-cloud-kms]
        set traffic-vdom {string}
        set gck-service-account {string}
        set gck-private-key {string}
        set gck-keyid {string}
        set gck-access-token-lifetime {integer}
    next
end
```

config system cloud-service

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
vendor	Cloud service vendor.	option	-	unknown
	Option		Description	
	<i>unknown</i>		Unknown type of cloud service vendor.	
	<i>google-cloud-kms</i>		Google Cloud KMS service.	
traffic-vdom	Vdom used to communicate with cloud service.	string	Maximum length: 31	
gck-service-account	Service account (e.g. "account-id@sampledomain.com").	string	Maximum length: 285	

Parameter	Description	Type	Size	Default
gck-private-key	Service account private key in PEM format (e.g. "-----BEGIN PRIVATE KEY-----\ ...").	string	Maximum length: 8191	
gck-keyid	Key id, also referred as "kid".	string	Maximum length: 127	
gck-access-token-lifetime	Lifetime of automatically generated access tokens in minutes (default is 60 minutes).	integer	Minimum value: 1 Maximum value: 3600	60

config system cmdb

System CMDB information.

```
config system cmdb
    Description: System CMDB information.
end
```

config system console

Configure console.

```
config system console
    Description: Configure console.
    set output [standard|more]
    set login [enable|disable]
end
```

config system console

Parameter	Description	Type	Size	Default
output	Console output mode.	option	-	more
	Option	Description		
	<i>standard</i>	Standard output.		
	<i>more</i>	More page output.		
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.		

config system csf

Add this FortiProxy to a Security Fabric or set up a new Security Fabric on this FortiProxy.

```
config system csf
    Description: Add this FortiProxy to a Security Fabric or set up a new Security Fabric on this
    FortiProxy.
    set status [enable|disable]
    set uid {string}
    set upstream {string}
    set source-ip {ipv4-address}
    set upstream-interface-select-method [auto|specify]
    set upstream-interface {string}
    set upstream-port {integer}
    set group-name {string}
    set group-password {password}
    set accept-auth-by-cert [disable|enable]
    set log-unification [disable|enable]
    set authorization-request-type [serial|certificate]
    set certificate {string}
    set fabric-workers {integer}
    set downstream-access [enable|disable]
    set license-sharing [enable|disable]
    set preferred-seats {integer}
    set legacy-authentication [disable|enable]
    set downstream-acprofile {string}
    set configuration-sync [default|local]
    set fabric-object-unification [default|local]
    set saml-configuration-sync [default|local]
    config trusted-list
        Description: Pre-authorized and blocked security fabric nodes.
        edit <name>
            set authorization-type [serial|certificate]
            set serial {string}
            set certificate {var-string}
            set action [accept|deny]
            set ha-members {string}
            set downstream-authorization [enable|disable]
            set preferred-seats {integer}
            set index {integer}
        next
    end
```

```

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 forticloud-account-enforcement [enable|disable]
set file-mgmt [enable|disable]
set file-quota {integer}
set file-quota-warning {integer}
end

```

config system csf

Parameter	Description	Type	Size	Default						
status	Enable/disable Security Fabric.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Security Fabric.</td></tr><tr><td><i>disable</i></td><td>Disable Security Fabric.</td></tr></table>				Option	Description	<i>enable</i>	Enable Security Fabric.	<i>disable</i>	Disable Security Fabric.
	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 FortiProxy upstream from this FortiProxy in the Security Fabric.	string	Maximum length: 255							
source-ip	Source IP address for communication with the upstream FortiGate.	ipv4-address	Not Specified	0.0.0.0						
upstream-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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
upstream-interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default						
upstream-port	The port number to use to communicate with the FortiProxy upstream from this FortiProxy in the Security Fabric (default = 8013).	integer	Minimum value: 1 Maximum value: 65535	8013						
group-name	Security Fabric group name. All FortiProxys 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							
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><i>disable</i></td><td>Do not accept SSL connections with unknown certificates.</td></tr><tr><td><i>enable</i></td><td>Accept SSL connections without automatic certificate verification.</td></tr></table>				Option	Description	<i>disable</i>	Do not accept SSL connections with unknown certificates.	<i>enable</i>	Accept SSL connections without automatic certificate verification.
Option	Description									
<i>disable</i>	Do not accept SSL connections with unknown certificates.									
<i>enable</i>	Accept SSL connections without automatic certificate verification.									
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.									
authorization-request-type	Authorization request type.	option	-	serial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>serial</i></td><td>Request verification by serial number.</td></tr><tr><td><i>certificate</i></td><td>Request verification by certificate.</td></tr></table>				Option	Description	<i>serial</i>	Request verification by serial number.	<i>certificate</i>	Request verification by certificate.
Option	Description									
<i>serial</i>	Request verification by serial number.									
<i>certificate</i>	Request verification by certificate.									
certificate	Certificate.	string	Maximum length: 35							
fabric-workers	Number of worker processes for Security Fabric daemon.	integer	Minimum value: 1 Maximum value: 4	2						

Parameter	Description	Type	Size	Default						
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><i>enable</i></td><td>Enable downstream device access to this device's configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable downstream device access to this device's configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable downstream device access to this device's configuration and data.	<i>disable</i>	Disable downstream device access to this device's configuration and data.			
Option	Description									
<i>enable</i>	Enable downstream device access to this device's configuration and data.									
<i>disable</i>	Disable downstream device access to this device's configuration and data.									
license-sharing	Enable/disable license sharing between FortiProxy devices.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable license sharing.</td></tr><tr><td><i>disable</i></td><td>Disable license sharing.</td></tr></table>	Option	Description	<i>enable</i>	Enable license sharing.	<i>disable</i>	Disable license sharing.			
Option	Description									
<i>enable</i>	Enable license sharing.									
<i>disable</i>	Disable license sharing.									
preferred-seats	The number of seats this FortiProxy device as CSF root should be allocated with. The number of gurrantted seats is capped by minimum of the number of local purchased seats and the number of preferred seats. And the rest of preferred seats will be allocated from shared pool at higher priority.	integer	Minimum value: 0 Maximum value: 4294967295	0						
legacy-authentication	Enable/disable legacy authentication.	option	-	enable						
	<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.									
downstream-accprofile	Default access profile for requests from downstream devices.	string	Maximum length: 35							
configuration-sync	Configuration sync mode.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.</td></tr><tr><td><i>local</i></td><td>Do not synchronize configuration with root node.</td></tr></table>	Option	Description	<i>default</i>	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.	<i>local</i>	Do not synchronize configuration with root node.			
Option	Description									
<i>default</i>	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.									
<i>local</i>	Do not synchronize configuration with root node.									

Parameter	Description	Type	Size	Default						
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Global CMDB objects will be synchronized in Security Fabric.</td></tr><tr><td><i>local</i></td><td>Global CMDB objects will not be synchronized to and from this device.</td></tr></table>	Option	Description	<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.	<i>local</i>	Global CMDB objects will not be synchronized to and from this device.			
Option	Description									
<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.									
<i>local</i>	Global CMDB objects will not be synchronized to and from this device.									
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.									
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.									
file-mgmt	Enable/disable Security Fabric daemon file management.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable daemon file management.</td></tr><tr><td><i>disable</i></td><td>Disable daemon file management.</td></tr></table>	Option	Description	<i>enable</i>	Enable daemon file management.	<i>disable</i>	Disable daemon file management.			
Option	Description									
<i>enable</i>	Enable daemon file management.									
<i>disable</i>	Disable daemon file management.									
file-quota	Maximum amount of memory that can be used by the daemon files (in bytes).	integer	Minimum value: 0 Maximum value: 4294967295	0						
file-quota-warning	Warn when the set percentage of quota has been used.	integer	Minimum value: 1 Maximum value: 99	90						

config trusted-list

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
authorization-type	Authorization type.	option	-	serial
	Option	Description		
	<i>serial</i>	Verify downstream by serial number.		
	<i>certificate</i>	Verify downstream by certificate.		
serial	Serial.	string	Maximum length: 19	
certificate	Certificate.	var-string	Maximum length: 32767	
action	Security fabric authorization action.	option	-	accept
	Option	Description		
	<i>accept</i>	Accept authorization request.		
	<i>deny</i>	Deny authorization request.		
ha-members	HA members.	string	Maximum length: 19	
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable downstream authorization.		
	<i>disable</i>	Disable downstream authorization.		
preferred-seats	The number of seats this FortiProxy device should be allocated with. The number of gurrantted seats is capped by minimum of the number of local purchased seats and the number of preferred seats. And the rest of preferred seats will be allocated from shared pool at higher priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
index	Index of the downstream in tree.	integer	Minimum value: 1 Maximum value: 1024	0

config fabric-connector

Parameter	Description	Type	Size	Default						
serial	Serial.	string	Maximum length: 19							
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.									
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 system custom-language

Configure custom languages.

```
config system custom-language
  Description: Configure custom languages.
  edit <name>
    set filename {string}
    set comments {var-string}
  next
end
```

config system custom-language

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
filename	Custom language file path.	string	Maximum length: 63	
comments	Comment.	var-string	Maximum length: 255	

config system ddns

Configure DDNS.

```
config system ddns
  Description: Configure DDNS.
  edit <ddnsid>
    set ddns-server [dyndns.org|dyns.net|...]
    set addr-type [ipv4|ipv6]
    set server-type [ipv4|ipv6]
    set ddns-server-addr <addr1>, <addr2>, ...
    set ddns-zone {string}
    set ddns-ttl {integer}
    set ddns-auth [disable|tsig]
    set ddns-keyname {string}
    set ddns-key {password_aes256}
    set ddns-domain {string}
    set ddns-username {string}
    set ddns-sn {string}
    set ddns-password {password}
    set use-public-ip [disable|enable]
    set update-interval {integer}
    set clear-text [disable|enable]
    set ssl-certificate {string}
    set bound-ip {string}
    set monitor-interface <interface-name1>, <interface-name2>, ...
  next
end
```

config system ddns

Parameter	Description	Type	Size	Default										
ddnsid	DDNS ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
ddns-server	Select a DDNS service provider.	option	-											
	<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></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			
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													

Parameter	Description	Type	Size	Default																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dipdns.net</td><td>dipdnsserver.dipdns.com</td></tr><tr><td>now.net.cn</td><td>ip.todayisp.com</td></tr><tr><td>dhs.org</td><td>members.dhs.org</td></tr><tr><td>easydns.com</td><td>members.easydns.com</td></tr><tr><td>genericDDNS</td><td>Generic DDNS based on RFC2136.</td></tr><tr><td>FortiGuardDDNS</td><td>FortiGuard DDNS service.</td></tr><tr><td>noip.com</td><td>dynupdate.no-ip.com</td></tr></table>		Option	Description	dipdns.net	dipdnsserver.dipdns.com	now.net.cn	ip.todayisp.com	dhs.org	members.dhs.org	easydns.com	members.easydns.com	genericDDNS	Generic DDNS based on RFC2136.	FortiGuardDDNS	FortiGuard DDNS service.	noip.com	dynupdate.no-ip.com			
	Option	Description																			
	dipdns.net	dipdnsserver.dipdns.com																			
	now.net.cn	ip.todayisp.com																			
	dhs.org	members.dhs.org																			
	easydns.com	members.easydns.com																			
	genericDDNS	Generic DDNS based on RFC2136.																			
	FortiGuardDDNS	FortiGuard DDNS service.																			
noip.com	dynupdate.no-ip.com																				
addr-type	Address type of interface address in DDNS update.	option	-	ipv4																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>Use IPv4 address of the interface.</td></tr><tr><td>ipv6</td><td>Use IPv6 address of the interface.</td></tr></table>		Option	Description	ipv4	Use IPv4 address of the interface.	ipv6	Use IPv6 address of the interface.													
	Option	Description																			
	ipv4	Use IPv4 address of the interface.																			
ipv6	Use IPv6 address of the interface.																				
server-type	Address type of the DDNS server.	option	-	ipv4																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>Use IPv4 addressing.</td></tr><tr><td>ipv6</td><td>Use IPv6 addressing.</td></tr></table>		Option	Description	ipv4	Use IPv4 addressing.	ipv6	Use IPv6 addressing.													
	Option	Description																			
	ipv4	Use IPv4 addressing.																			
ipv6	Use IPv6 addressing.																				
ddns-server-addr <addr>	Generic DDNS server IP/FQDN list. IP address or FQDN of the server.	string	Maximum length: 256																		
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64																		
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 60 Maximum value: 86400	300																	
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-	disable																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DDNS authentication.</td></tr><tr><td>tsig</td><td>Enable TSIG authentication based on RFC2845.</td></tr></table>		Option	Description	disable	Disable DDNS authentication.	tsig	Enable TSIG authentication based on RFC2845.													
	Option	Description																			
	disable	Disable DDNS authentication.																			
tsig	Enable TSIG authentication based on RFC2845.																				

Parameter	Description	Type	Size	Default						
ddns-keyname	DDNS update key name.	string	Maximum length: 64							
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified							
ddns-domain	Your fully qualified domain name. For example, yourname.ddns.com.	string	Maximum length: 64							
ddns-username	DDNS user name.	string	Maximum length: 64							
ddns-sn	DDNS Serial Number.	string	Maximum length: 64							
ddns-password	DDNS password.	password	Not Specified							
use-public-ip	Enable/disable use of public IP address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of public IP address.</td></tr><tr><td>enable</td><td>Enable use of public IP address.</td></tr></table>				Option	Description	disable	Disable use of public IP address.	enable	Enable use of public IP address.
Option	Description									
disable	Disable use of public IP address.									
enable	Enable use of public IP address.									
update-interval	DDNS update interval (60 - 2592000 sec, 0 means default).	integer	Minimum value: 60 Maximum value: 2592000	0						
clear-text	Enable/disable use of clear text connections.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of clear text connections.</td></tr><tr><td>enable</td><td>Enable use of clear text connections.</td></tr></table>				Option	Description	disable	Disable use of clear text connections.	enable	Enable use of clear text connections.
Option	Description									
disable	Disable use of clear text connections.									
enable	Enable use of clear text connections.									
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
bound-ip	Bound IP address.	string	Maximum length: 46							
monitor-interface <interface-name>	Monitored interface. Interface name.	string	Maximum length: 79							

config system device-upgrade

Independent upgrades for managed devices.

```
config system device-upgrade
  Description: Independent upgrades for managed devices.
  edit <serial>
    set timing [immediate|scheduled]
    set maximum-minutes {integer}
    set time {user}
    set setup-time {user}
    set upgrade-path {user}
    set device-type [fortiproxy|fortiswitch|...]
    set status [disabled|initialized|...]
    set failure-reason [none|internal|...]
    set ha-reboot-controller {string}
    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
    next
  end
end
```

config system device-upgrade

Parameter	Description	Type	Size	Default
serial	Serial number of the node to include.	string	Maximum length: 79	
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.		
maximum-minutes	Maximum number of minutes to allow for immediate upgrade preparation.	integer	Minimum value: 5 Maximum value: 10080	15
time	Scheduled upgrade execution time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	

Parameter	Description	Type	Size	Default
setup-time	Upgrade preparation start time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
upgrade-path	Fortinet OS image versions to upgrade through in major-minor-patch format, such as 7-0-4.	user	Not Specified	
device-type	Fortinet device type.	option	-	fortiproxy
	Option Description			
	fortiproxy	This device is a FortiProxy.		
	fortiswitch	This device is a FortiSwitch.		
	fortiap	This device is a FortiAP.		
	fortiextender	This device is a FortiExtender.		
status	Current status of the upgrade.	option	-	disabled
	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.		
	upgrade-devices	The upgrade is ready and devices are being rebooted.		
	cancelled	The upgrade was cancelled due to the tree not being ready.		
	confirmed	The upgrade was confirmed and reboots are running.		
	done	The upgrade completed successfully.		
failed	The upgrade failed due to a local issue.			
failure-reason	Upgrade failure reason.	option	-	none

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No failure.</td></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 FortiProxy</td></tr><tr><td><i>node-failed</i></td><td>A device in the Security Fabric tree failed.</td></tr></table>	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 FortiProxy	<i>node-failed</i>	A device in the Security Fabric tree failed.			
	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 FortiProxy																																				
<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																																			

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 status [disable|enable]
    set lease-time {integer}
    set mac-acl-default-action [assign|block]
    set forticlient-on-net-status [disable|enable]
    set dns-service [local|default|...]
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-server3 {ipv4-address}
    set dns-server4 {ipv4-address}
    set wifi-ac-service [specify|local]
    set wifi-ac1 {ipv4-address}
    set wifi-ac2 {ipv4-address}
    set wifi-ac3 {ipv4-address}
    set ntp-service [local|default|...]
    set ntp-server1 {ipv4-address}
    set ntp-server2 {ipv4-address}
    set ntp-server3 {ipv4-address}
    set domain {string}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
    set default-gateway {ipv4-address}
    set next-server {ipv4-address}
    set netmask {ipv4-netmask}
    set interface {string}
  config ip-range
    Description: DHCP IP range configuration.
    edit <id>
      set start-ip {ipv4-address}
      set end-ip {ipv4-address}
      set vci-match [disable|enable]
      set vci-string <vci-string1>, <vci-string2>, ...
      set uci-match [disable|enable]
      set uci-string <uci-string1>, <uci-string2>, ...
      set lease-time {integer}
    next
  end
  set timezone-option [disable|default|...]
  set timezone {string}
  set tftp-server <tftp-server1>, <tftp-server2>, ...
  set filename {string}
  config options
    Description: DHCP options.
    edit <id>
      set code {integer}
```

```

        set type [hex|string|...]
        set value {string}
        set ip {user}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
        set uci-match [disable|enable]
        set uci-string <uci-string1>, <uci-string2>, ...
    next
end
set server-type [regular|ipsec]
set ip-mode [range|usrgrp]
set conflicted-ip-timeout {integer}
set ipsec-lease-hold {integer}
set auto-configuration [disable|enable]
set dhcp-settings-from-fortiipam [disable|enable]
set auto-managed-status [disable|enable]
set ddns-update [disable|enable]
set ddns-update-override [disable|enable]
set ddns-server-ip {ipv4-address}
set ddns-zone {string}
set ddns-auth [disable|tsig]
set ddns-keyname {string}
set ddns-key {password_aes256}
set ddns-ttl {integer}
set vci-match [disable|enable]
set vci-string <vci-string1>, <vci-string2>, ...
config exclude-range
    Description: Exclude one or more ranges of IP addresses from being assigned to
clients.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
        set uci-match [disable|enable]
        set uci-string <uci-string1>, <uci-string2>, ...
        set lease-time {integer}
    next
end
set shared-subnet [disable|enable]
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 type [mac|option82]
        set ip {ipv4-address}
        set mac {mac-address}
        set action [assign|block|...]
        set circuit-id-type [hex|string]
        set circuit-id {string}
        set remote-id-type [hex|string]

```

```

        set remote-id {string}
        set description {var-string}
    next
end
next
end

```

config system dhcp server

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>assign</i></td><td>Allow the DHCP server to assign IP settings to clients on the MAC access control list.</td></tr><tr><td><i>block</i></td><td>Block the DHCP server from assigning IP settings to clients on the MAC access control list.</td></tr></table>	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.			
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.									
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiClient On-Net Status.</td></tr><tr><td><i>enable</i></td><td>Enable FortiClient On-Net Status.</td></tr></table>	Option	Description	<i>disable</i>	Disable FortiClient On-Net Status.	<i>enable</i>	Enable FortiClient On-Net Status.			
Option	Description									
<i>disable</i>	Disable FortiClient On-Net Status.									
<i>enable</i>	Enable FortiClient On-Net Status.									

Parameter	Description	Type	Size	Default								
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local</i></td><td>IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.</td></tr><tr><td><i>default</i></td><td>Clients are assigned the FortiProxy's configured DNS servers.</td></tr><tr><td><i>specify</i></td><td>Specify up to 3 DNS servers in the DHCP server configuration.</td></tr></table>	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 FortiProxy's configured DNS servers.	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.			
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 FortiProxy's configured DNS servers.											
<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.											
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								
wifi-ac-service	Options for assigning WiFi access controllers to DHCP clients.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>specify</i></td><td>Specify up to 3 WiFi Access Controllers in the DHCP server configuration.</td></tr><tr><td><i>local</i></td><td>IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.</td></tr></table>	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.					
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								
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local</i></td><td>IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.</td></tr></table>	Option	Description	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.							
Option	Description											
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Clients are assigned the FortiProxy's configured NTP servers.		
	<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.		
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
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35	
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
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	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
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified	0.0.0.0
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15	
timezone-option	Options for the DHCP server to set the client's time zone.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not set the client's time zone.		
	<i>default</i>	Clients are assigned the FortiProxy's configured time zone.		
	<i>specify</i>	Specify the time zone to be assigned to DHCP clients.		
timezone	Select the time zone to be assigned to DHCP clients.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
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							
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127							
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-	regular						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>Regular DHCP service.</td></tr><tr><td><i>ipsec</i></td><td>DHCP over IPsec service.</td></tr></table>				Option	Description	<i>regular</i>	Regular DHCP service.	<i>ipsec</i>	DHCP over IPsec service.
Option	Description									
<i>regular</i>	Regular DHCP service.									
<i>ipsec</i>	DHCP over IPsec service.									
ip-mode	Method used to assign client IP.	option	-	range						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>range</i></td><td>Use range defined by start-ip/end-ip to assign client IP.</td></tr><tr><td><i>usrgrp</i></td><td>Use user-group defined method to assign client IP.</td></tr></table>				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.
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.									
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						
ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 0 Maximum value: 8640000	60						
auto-configuration	Enable/disable auto configuration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable auto configuration.</td></tr><tr><td><i>enable</i></td><td>Enable auto configuration.</td></tr></table>				Option	Description	<i>disable</i>	Disable auto configuration.	<i>enable</i>	Enable auto configuration.
Option	Description									
<i>disable</i>	Disable auto configuration.									
<i>enable</i>	Enable auto configuration.									
dhcp-settings-from-fortiipam	Enable/disable populating of DHCP server settings from FortiIPAM.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable populating of DHCP server settings from FortiIPAM.		
	<i>enable</i>	Enable populating of DHCP server settings from FortiIPAM.		
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.		
ddns-update	Enable/disable DDNS update for DHCP.	option	-	disable
	Option Description			
	<i>disable</i>	Disable DDNS update for DHCP.		
	<i>enable</i>	Enable DDNS update for DHCP.		
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-	disable
	Option Description			
	<i>disable</i>	Disable DDNS update override for DHCP.		
	<i>enable</i>	Enable DDNS update override for DHCP.		
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified	0.0.0.0
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64	
ddns-auth	DDNS authentication mode.	option	-	disable
	Option Description			
	<i>disable</i>	Disable DDNS authentication.		
	<i>tsig</i>	TSIG based on RFC2845.		
ddns-keyname	DDNS update key name.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified	
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400	300
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	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	
shared-subnet	Enable/disable shared subnet.	option	-	disable
	Option		Description	
	<i>disable</i>		Disable shared subnet.	
	<i>enable</i>		Enable shared subnet.	
relay-agent	Relay agent IP.	ipv4-address	Not Specified	0.0.0.0

config ip-range

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

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						
	<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							
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							
lease-time	Lease time in seconds, 0 means default lease time.	integer	Minimum value: 300 Maximum value: 8640000	0						

config options

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default										
type	DHCP option type.	option	-	hex										
	<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><tr><td>ip</td><td>DHCP option in IP.</td></tr><tr><td>fqdn</td><td>DHCP option in domain search option format.</td></tr></table>	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.			
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 option value.	string	Maximum length: 312											
ip	DHCP option IPs.	user	Not Specified											
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											
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										
	<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											

config exclude-range

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0						
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0						
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						
	<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							
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><i>disable</i></td><td>Disable UCI matching.</td></tr><tr><td><i>enable</i></td><td>Enable UCI matching.</td></tr></table>				Option	Description	<i>disable</i>	Disable UCI matching.	<i>enable</i>	Enable UCI matching.
Option	Description									
<i>disable</i>	Disable UCI matching.									
<i>enable</i>	Enable UCI matching.									
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255							
lease-time	Lease time in seconds, 0 means default lease time.	integer	Minimum value: 300 Maximum value: 8640000	0						

config reserved-address

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	DHCP reserved-address type.	option	-	mac
	Option	Description		
	<i>mac</i>	Match with MAC address.		
	<i>option82</i>	Match with DHCP option 82.		
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
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-type	DHCP option type.	option	-	string
	Option	Description		
	<i>hex</i>	DHCP option in hex.		
	<i>string</i>	DHCP option in string.		
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
remote-id-type	DHCP option type.	option	-	string

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>hex</i>	DHCP option in hex.		
	<i>string</i>	DHCP option in string.		
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
description	Description.	var-string	Maximum length: 255	

config system dhcp6 server

Configure DHCPv6 servers.

```

config system dhcp6 server
  Description: Configure DHCPv6 servers.
  edit <id>
    set status [disable|enable]
    set rapid-commit [disable|enable]
    set lease-time {integer}
    set dns-service [delegated|default|...]
    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 domain {string}
    set subnet {ipv6-prefix}
    set interface {string}
    set option1 {user}
    set option2 {user}
    set option3 {user}
    set upstream-interface {string}
    set delegated-prefix-iaid {integer}
    set ip-mode [range|delegated]
    set prefix-mode [dhcp6|ra]
    config prefix-range
      Description: DHCP prefix configuration.
      edit <id>
        set start-prefix {ipv6-address}
        set end-prefix {ipv6-address}
        set prefix-length {integer}
      next
    end
  config ip-range
    Description: DHCP IP range configuration.
```

```

        edit <id>
            set start-ip {ipv6-address}
            set end-ip {ipv6-address}
        next
    end
next
end

```

config system dhcp6 server

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.		
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.		
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-	specify
	Option	Description		
	<i>delegated</i>	Delegated DNS settings.		
	<i>default</i>	Clients are assigned the FortiProxy's configured DNS servers.		
	<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.		

Parameter	Description	Type	Size	Default						
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	::						
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35							
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified	::/0						
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15							
option1	Option 1.	user	Not Specified							
option2	Option 2.	user	Not Specified							
option3	Option 3.	user	Not Specified							
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15							
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-mode	Method used to assign client IP.	option	-	range						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>range</i></td><td>Use range defined by start IP/end IP to assign client IP.</td></tr><tr><td><i>delegated</i></td><td>Use delegated prefix method to assign client IP.</td></tr></table>	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.			
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.									

Parameter	Description	Type	Size	Default						
prefix-mode	Assigning a prefix from a DHCPv6 client or RA.	option	-	dhcp6						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dhcp6</td><td>Use delegated prefix from a DHCPv6 client.</td></tr><tr><td>ra</td><td>Use prefix from RA.</td></tr></table>	Option	Description	dhcp6	Use delegated prefix from a DHCPv6 client.	ra	Use prefix from RA.			
Option	Description									
dhcp6	Use delegated prefix from a DHCPv6 client.									
ra	Use prefix from RA.									

config prefix-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-prefix	Start of prefix range.	ipv6-address	Not Specified	::
end-prefix	End of prefix range.	ipv6-address	Not Specified	::
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128	0

config ip-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IP range.	ipv6-address	Not Specified	::
end-ip	End of IP range.	ipv6-address	Not Specified	::

config system dns

Configure DNS.

```

config system dns
    Description: Configure DNS.
    set primary {ipv4-address}
    set secondary {ipv4-address}
    set protocol {option1}, {option2}, ...
    set ssl-certificate {string}
    set server-hostname <hostname1>, <hostname2>, ...
    set domain <domain1>, <domain2>, ...
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set timeout {integer}
    set retry {integer}
    set dns-cache-limit {integer}
    set dns-cache-ttl {integer}
    set cache-notfound-responses [disable|enable]
    set source-ip {ipv4-address}
    set interface-select-method [auto|specify]
    set interface {string}
    set server-select-method [least-rtt|failover]
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
    set log [disable|error|...]
    set fqdn-cache-ttl {integer}
    set fqdn-max-refresh {integer}
    set fqdn-min-refresh {integer}
end

```

config system dns

Parameter	Description	Type	Size	Default								
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0								
secondary	Secondary 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><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.											
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory								

Parameter	Description	Type	Size	Default						
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127							
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127							
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified	::						
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified	::						
timeout	DNS query timeout interval in seconds (1 - 10).	integer	Minimum value: 1 Maximum value: 10	5						
retry	Number of times to retry (0 - 5).	integer	Minimum value: 0 Maximum value: 5	2						
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						
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><i>disable</i></td><td>Disable cache NOTFOUND responses from DNS server.</td></tr><tr><td><i>enable</i></td><td>Enable cache NOTFOUND responses from DNS server.</td></tr></table>				Option	Description	<i>disable</i>	Disable cache NOTFOUND responses from DNS server.	<i>enable</i>	Enable cache NOTFOUND responses from DNS server.
Option	Description									
<i>disable</i>	Disable cache NOTFOUND responses from DNS server.									
<i>enable</i>	Enable cache NOTFOUND responses from DNS server.									
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified	0.0.0.0						
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>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt
	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.		
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
log	Local DNS log setting.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>error</i>	Enable local DNS error log.		
	<i>all</i>	Enable local DNS log.		
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
fqdn-min-refresh	FQDN cache minimum refresh time in seconds (10 - 3600, default = 60).	integer	Minimum value: 10 Maximum value: 3600	60

config system dns-database

Configure DNS databases.

```
config system dns-database
  Description: Configure DNS databases.
  edit <name>
    set status [enable|disable]
    set domain {string}
    set allow-transfer {user}
    set type [primary|secondary]
    set view [shadow|public|...]
    set ip-primary {ipv4-address-any}
    set primary-name {string}
    set contact {string}
    set ttl {integer}
    set authoritative [enable|disable]
    set forwarder {user}
    set forwarder6 {ipv6-address}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set rr-max {integer}
  config dns-entry
    Description: DNS entry.
    edit <id>
      set status [enable|disable]
      set type [A|NS|...]
      set ttl {integer}
      set preference {integer}
      set ip {ipv4-address-any}
      set ipv6 {ipv6-address}
      set hostname {string}
      set canonical-name {string}
    next
  end
next
end
```

config system dns-database

Parameter	Description	Type	Size	Default
name	Zone name.	string	Maximum length: 35	
status	Enable/disable this DNS zone.	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.													
domain	Domain name.	string	Maximum length: 255											
allow-transfer	DNS zone transfer IP address list.	user	Not Specified											
type	Zone type (primary to manage entries directly, secondary to import entries from other zones).	option	-	primary										
	<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.													
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										
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255	dns										
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										

Parameter	Description	Type	Size	Default						
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						
authoritative	Enable/disable authoritative zone.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authoritative zone.</td></tr><tr><td><i>disable</i></td><td>Disable authoritative zone.</td></tr></table>				Option	Description	<i>enable</i>	Enable authoritative zone.	<i>disable</i>	Disable authoritative zone.
Option	Description									
<i>enable</i>	Enable authoritative zone.									
<i>disable</i>	Disable authoritative zone.									
forwarder	DNS zone forwarder IP address list.	user	Not Specified							
forwarder6	Forwarder IPv6 address.	ipv6-address	Not Specified	::						
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	IPv6 source IP address for forwarding to DNS server.	ipv6-address	Not Specified	::						
rr-max	Maximum number of resource records (10 - 65536, 0 means infinite).	integer	Minimum value: 10 Maximum value: 65536	16384						

config dns-entry

Parameter	Description	Type	Size	Default						
id	DNS entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable resource record status.	option	-	enable						
	<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.									
type	Resource record type.	option	-	A						

Parameter	Description	Type	Size	Default																
	<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.																			
ttl	Time-to-live for this entry (0 to 2147483647 sec, default = 0).	integer	Minimum value: 0 Maximum value: 2147483647	0																
preference	DNS entry preference (0 - 65535, highest preference = 0, default = 10).	integer	Minimum value: 0 Maximum value: 65535	10																
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	::																
hostname	Name of the host.	string	Maximum length: 255																	
canonical-name	Canonical name of the host.	string	Maximum length: 255																	

config system dns-server

Configure DNS servers.

```
config system dns-server
  Description: Configure DNS servers.
  edit <name>
    set mode [recursive|non-recursive|...]
    set dnsfilter-profile {string}
    set doh [enable|disable]
    set doh3 [enable|disable]
    set doq [enable|disable]
```



```
next
end
```

config system dns-server

Parameter	Description	Type	Size	Default
name	DNS server name.	string	Maximum length: 15	
mode	DNS server mode.	option	-	recursive
	Option	Description		
	<i>recursive</i>	Shadow DNS database and forward.		
	<i>non-recursive</i>	Public DNS database only.		
	<i>forward-only</i>	Forward only.		
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35	
doh	Enable/disable DNS over HTTPS/443 (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS over HTTPS.		
	<i>disable</i>	Disable DNS over HTTPS.		
doh3	Enable/disable DNS over QUIC/HTTP3/443 (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS over HTTP3/QUIC.		
	<i>disable</i>	Disable DNS over HTTP3/QUIC.		
doq	Enable/disable DNS over QUIC/853 (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS over QUIC.		
	<i>disable</i>	Disable DNS over QUIC.		

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								
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
ds	DSCP(DiffServ) DS value (0 - 63).	integer	Minimum value: 0 Maximum value: 63	0								
priority	DSCP based priority level.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Low priority.</td></tr><tr><td><i>medium</i></td><td>Medium priority.</td></tr><tr><td><i>high</i></td><td>High priority.</td></tr></table>				Option	Description	<i>low</i>	Low priority.	<i>medium</i>	Medium priority.	<i>high</i>	High priority.
Option	Description											
<i>low</i>	Low priority.											
<i>medium</i>	Medium priority.											
<i>high</i>	High priority.											

config system email-server

Configure the email server used by the FortiProxy 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 FortiProxy various things. For example,
    for sending email messages to users to support user authentication features.
    set type {option}
    set server {string}
    set port {integer}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set authenticate [enable|disable]
    set validate-server [enable|disable]
    set username {string}

```

```

set password {password}
set security [none|starttls|...]
set ssl-min-proto-version [default|SSLv3|...]
set interface-select-method [auto|specify]
set interface {string}
end

```

config system email-server

Parameter	Description	Type	Size	Default
type	Use FortiGuard Message service or custom email server.	option	-	custom
	Option Description			
	<i>custom</i>	Use custom email server.		
server	SMTP server IP address or hostname.	string	Maximum length: 63	
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535	25
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	::
authenticate	Enable/disable authentication.	option	-	disable
	Option Description			
	<i>enable</i>	Enable authentication.		
	<i>disable</i>	Disable authentication.		
validate-server	Enable/disable validation of server certificate.	option	-	disable
	Option Description			
	<i>enable</i>	Enable validation of server certificate.		
	<i>disable</i>	Disable validation of server certificate.		
username	SMTP server user name for authentication.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default														
password	SMTP server user password for authentication.	password	Not Specified															
security	Connection security used by the email server.	option	-	none														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>starttls</i></td><td>STARTTLS.</td></tr><tr><td><i>smtps</i></td><td>SSL/TLS.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>starttls</i>	STARTTLS.	<i>smtps</i>	SSL/TLS.									
Option	Description																	
<i>none</i>	None.																	
<i>starttls</i>	STARTTLS.																	
<i>smtps</i>	SSL/TLS.																	
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.																	
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.											
Option	Description																	
<i>auto</i>	Set outgoing interface automatically.																	
<i>specify</i>	Set outgoing interface manually.																	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15															

config system external-resource

Configure external resource.

```
config system external-resource
    Description: Configure external resource.
    edit <name>
        set uuid {uuid}
```

```

set status [enable|disable]
set type [category|domain|...]
set update-method [feed|push]
set category {integer}
set username {string}
set password {password}
set comments {var-string}
set resource {string}
set user-agent {var-string}
set proxy {string}
set proxy-port {integer}
set proxy-username {string}
set proxy-password {password}
set server-identity-check [none|basic|...]
set refresh-rate {integer}
set source-ip {ipv4-address}
set interface-select-method [auto|specify]
set interface {string}
next
end

```

config system external-resource

Parameter	Description	Type	Size	Default										
name	External resource name.	string	Maximum length: 35											
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000										
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></table>				Option	Description	<i>category</i>	FortiGuard category.	<i>domain</i>	Domain Name.	<i>malware</i>	Malware hash.	<i>address</i>	Firewall IP address.
Option	Description													
<i>category</i>	FortiGuard category.													
<i>domain</i>	Domain Name.													
<i>malware</i>	Malware hash.													
<i>address</i>	Firewall IP address.													

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>data</i></td><td>Data file.</td></tr><tr><td><i>url</i></td><td>URL List.</td></tr></table>				Option	Description	<i>data</i>	Data file.	<i>url</i>	URL List.
	Option	Description								
	<i>data</i>	Data file.								
<i>url</i>	URL List.									
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.									
category	User resource category.	integer	Minimum value: 192 Maximum value: 221	0						
username	HTTP basic authentication user name.	string	Maximum length: 64							
password	HTTP basic authentication password.	password	Not Specified							
comments	Comment.	var-string	Maximum length: 255							
resource	URL of external resource.	string	Maximum length: 511							
user-agent	HTTP User-Agent header (default = 'curl/7.58.0').	var-string	Maximum length: 255							
proxy	Proxy server host(ip or domain name).	string	Maximum length: 255							
proxy-port	Port number that the proxy server expects to receive HTTP sessions on (1 - 65535, default = 8080).	integer	Minimum value: 1 Maximum value: 65535	8080						
proxy-username	HTTP proxy basic authentication user name.	string	Maximum length: 64							
proxy-password	HTTP proxy basic authentication password.	password	Not Specified							

Parameter	Description	Type	Size	Default								
server-identity-check	Certificate verification option.	option	-	none								
	<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 certficate 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 certficate 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 certficate only.											
<i>full</i>	Check server certificate and verify the domain matches in the server certificate.											
refresh-rate	Time interval to refresh external resource (1 - 43200 min, default = 5 min).	integer	Minimum value: 1 Maximum value: 43200	5								
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0								
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.					
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

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.
  set status [enable|disable]
  set sync-mode [enable|disable]
  set branch-name {string}
  set policy-rule [health-check|manual|...]
  set vpn-role [hub|spoke]
  config overlays
    Description: Local overlay interfaces table.
    edit <name>
      set overlay-tunnel-block {ipv4-classnet-host}

```

```

        set remote-gw {ipv4-address-any}
        set interface {string}
        set bgp-neighbor {string}
        set overlay-policy {integer}
        set bgp-network {integer}
        set route-policy {integer}
        set bgp-neighbor-group {string}
        set bgp-neighbor-range {integer}
        set ipsec-phase1 {string}
        set sdwan-member {integer}
    next
end
config advertised-subnets
    Description: Local advertised subnets.
    edit <id>
        set prefix {ipv4-classnet}
        set access [inbound|bidirectional]
        set bgp-network {integer}
        set firewall-address {string}
        set policies {integer}
    next
end
set loopback-address-block {ipv4-classnet-host}
set loopback-interface {string}
set loopback-advertised-subnet {integer}
set psksecret {password-3}
set bgp-as {integer}
set sdwan-zone {string}
set health-checks {string}
end

```

config system fabric-vpn

Parameter	Description	Type	Size	Default
status	Enable/disable Fabric VPN.	option	-	disable
	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.		

Parameter	Description	Type	Size	Default								
branch-name	Branch name.	string	Maximum length: 35									
policy-rule	Policy creation rule.	option	-	health-check								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>health-check</i></td><td>Create health check policy automatically.</td></tr><tr><td><i>manual</i></td><td>All policies will be created manually.</td></tr><tr><td><i>auto</i></td><td>Automatically create allow policies.</td></tr></table>				Option	Description	<i>health-check</i>	Create health check policy automatically.	<i>manual</i>	All policies will be created manually.	<i>auto</i>	Automatically create allow policies.
	Option	Description										
	<i>health-check</i>	Create health check policy automatically.										
	<i>manual</i>	All policies will be created manually.										
<i>auto</i>	Automatically create allow policies.											
vpn-role	Fabric VPN role.	option	-	hub								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hub</i></td><td>VPN hub.</td></tr><tr><td><i>spoke</i></td><td>VPN spoke.</td></tr></table>				Option	Description	<i>hub</i>	VPN hub.	<i>spoke</i>	VPN spoke.		
	Option	Description										
	<i>hub</i>	VPN hub.										
<i>spoke</i>	VPN spoke.											
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-interface	Loopback interface.	string	Maximum length: 15									
loopback-advertised-subnet	Loopback advertised subnet reference.	integer	Minimum value: 0 Maximum value: 4294967295	0								
psksecret	Pre-shared secret for ADVPN.	password-3	Not Specified									
bgp-as	BGP Router AS number, valid from 1 to 4294967295.	integer	Minimum value: 0 Maximum value: 4294967295	0								
sdwan-zone	Reference to created SD-WAN zone.	string	Maximum length: 35									
health-checks	Underlying health checks.	string	Maximum length: 35									

config overlays

Parameter	Description	Type	Size	Default
name	Overlay name.	string	Maximum length: 79	
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
interface	Underlying interface name.	string	Maximum length: 15	
bgp-neighbor	Underlying BGP neighbor entry.	string	Maximum length: 45	
overlay-policy	The overlay policy to allow ADVPN thru traffic.	integer	Minimum value: 0 Maximum value: 4294967295	0
bgp-network	Underlying BGP network.	integer	Minimum value: 0 Maximum value: 4294967295	0
route-policy	Underlying router policy.	integer	Minimum value: 0 Maximum value: 4294967295	0
bgp-neighbor-group	Underlying BGP neighbor group entry.	string	Maximum length: 45	
bgp-neighbor-range	Underlying BGP neighbor range entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
ipsec-phase1	IPsec interface.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
sdwan-member	Reference to SD-WAN member entry.	integer	Minimum value: 0 Maximum value: 4294967295	0

config advertised-subnets

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967294	0						
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
access	Access policy direction.	option	-	inbound						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inbound</i></td><td>Allow inbound traffic to subnet.</td></tr><tr><td><i>bidirectional</i></td><td>Allow inbound and outbound traffic to subnet.</td></tr></table>				Option	Description	<i>inbound</i>	Allow inbound traffic to subnet.	<i>bidirectional</i>	Allow inbound and outbound traffic to subnet.
	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 Maximum value: 4294967295	0						
firewall-address	Underlying firewall address.	string	Maximum length: 79							
policies	Underlying policies.	integer	Minimum value: 0 Maximum value: 4294967295							

config system federated-upgrade

Coordinate federated upgrades within the Security Fabric.

```
config system federated-upgrade
  Description: Coordinate federated upgrades within the Security Fabric.
  set status [disabled|initialized|...]
```

```

set source [user|auto-firmware-upgrade]
set failure-reason [none|internal|...]
set failure-device {string}
set upgrade-id {integer}
set next-path-index {integer}
set ha-reboot-controller {string}
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
config node-list
    Description: Nodes which will be included in the upgrade.
    edit <serial>
        set timing [immediate|scheduled]
        set maximum-minutes {integer}
        set time {user}
        set setup-time {user}
        set upgrade-path {user}
        set device-type [fortiproxy|fortiswitch|...]
        set coordinating-fortiproxy {string}
    next
end
end

```

config system federated-upgrade

Parameter	Description	Type	Size	Default
status	Current status of the upgrade.	option	-	disabled
	Option	Description		
	<i>disabled</i>	No federated upgrade has been configured.		
	<i>initialized</i>	The upgrade has been configured.		
	<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.		

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>failed</i>	The upgrade failed due to a local issue.		
	source	Source that set up the federated upgrade config.	option	-
	Option	Description		
	<i>user</i>	Upgrade configured based on user input.		
	<i>auto-firmware-upgrade</i>	Upgrade configured by the FortiGuard auto-firmware-upgrade feature.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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 FortiProxy		
	<i>node-failed</i>	A device in the Security Fabric tree failed.		
failure-device	Serial number of the node to include.	string	Maximum length: 79	
upgrade-id	Unique identifier for this upgrade.	integer	Minimum value: 0 Maximum value: 4294967295	0
next-path-index	The index of the next image to upgrade to.	integer	Minimum value: 0 Maximum value: 10	0
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	

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
serial	Serial number of the node to include.	string	Maximum length: 79	
timing	Run immediately or at a scheduled time.	option	-	immediate

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>immediate</i>	Begin the upgrade immediately.		
	<i>scheduled</i>	Begin the upgrade at a configured time.		
maximum-minutes	Maximum number of minutes to allow for immediate upgrade preparation.	integer	Minimum value: 5 Maximum value: 10080	15
time	Scheduled upgrade execution time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
setup-time	Upgrade preparation start time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
upgrade-path	Fortinet OS image versions to upgrade through in major-minor-patch format, such as 7-0-4.	user	Not Specified	
device-type	Fortinet device type.	option	-	fortiproxy
	Option	Description		
	<i>fortiproxy</i>	This device is a FortiProxy.		
	<i>fortiswitch</i>	This device is a FortiSwitch.		
	<i>fortiap</i>	This device is a FortiAP.		
	<i>fortiextender</i>	This device is a FortiExtender.		
coordinating-fortiproxy	Serial number of the FortiGate unit that controls this device.	string	Maximum length: 79	

config system fips-cc

Configure FIPS-CC mode.

```
config system fips-cc
  Description: Configure FIPS-CC mode.
  set status [enable|disable]
  set self-test-period {integer}
  set key-generation-self-test [enable|disable]
end
```

config system fips-cc

Parameter	Description	Type	Size	Default
status	Enable/disable ciphers for FIPS mode of operation.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FIPS-CC mode.		
	<i>disable</i>	Disable FIPS-CC mode.		
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440	1440
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.		

config system fortianalyzer-connectivity

FortiAnalyzer Connectivity.

```
config system fortianalyzer-connectivity
  Description: FortiAnalyzer Connectivity.
end
```

config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
  Description: Configure FortiGuard services.
  set fortiguard-anycast [enable|disable]
  set fortiguard-anycast-source [fortinet|aws|...]
  set protocol [udp|http|...]
  set port [8888|53|...]
  set service-account-id {string}
  set load-balance-servers {integer}
```



```

set auto-join-forticloud [enable|disable]
set update-server-location [automatic|usa|...]
set sandbox-region {string}
set sandbox-inline-scan [enable|disable]
set update-ffdb [enable|disable]
set update-uwdb [enable|disable]
set update-dldb [enable|disable]
set update-extdb [enable|disable]
set update-build-proxy [enable|disable]
set persistent-connection [enable|disable]
set vdom {string}
set auto-firmware-upgrade [enable|disable]
set auto-firmware-upgrade-day {option1}, {option2}, ...
set auto-firmware-upgrade-delay {integer}
set auto-firmware-upgrade-start-hour {integer}
set auto-firmware-upgrade-end-hour {integer}
set FDS-license-expiring-days {integer}
set antispam-force-off [enable|disable]
set antispam-cache [enable|disable]
set antispam-cache-ttl {integer}
set antispam-cache-mpermille {integer}
set antispam-license {integer}
set antispam-expiration {integer}
set antispam-timeout {integer}
set outbreak-prevention-force-off [enable|disable]
set outbreak-prevention-cache [enable|disable]
set outbreak-prevention-cache-ttl {integer}
set outbreak-prevention-cache-mpermille {integer}
set outbreak-prevention-license {integer}
set outbreak-prevention-expiration {integer}
set outbreak-prevention-timeout {integer}
set fnbi-license {integer}
set fnbi-expiration {integer}
set webfilter-force-off [enable|disable]
set webfilter-cache [enable|disable]
set webfilter-cache-ttl {integer}
set webfilter-license {integer}
set webfilter-expiration {integer}
set webfilter-timeout {integer}
set sdns-server-ip {user}
set sdns-server-port {integer}
set anycast-sdns-server-ip {ipv4-address}
set anycast-sdns-server-port {integer}
set sdns-options {option1}, {option2}, ...
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set proxy-server-ip {string}
set proxy-server-port {integer}
set proxy-username {string}
set proxy-password {password}
set ddns-server-ip {ipv4-address}
set ddns-server-ip6 {ipv6-address}

```

```

set ddns-server-port {integer}
set interface-select-method [auto|specify]
set interface {string}
end

```

config system fortiguard

Parameter	Description	Type	Size	Default								
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of FortiGuard's Anycast network.</td></tr><tr><td><i>disable</i></td><td>Disable use of FortiGuard's Anycast network.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of FortiGuard's Anycast network.	<i>disable</i>	Disable use of FortiGuard's Anycast network.					
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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortinet</i></td><td>Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.</td></tr><tr><td><i>aws</i></td><td>Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.</td></tr><tr><td><i>debug</i></td><td>Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.</td></tr></table>	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.			
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.											
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).											
port	Port used to communicate with the FortiGuard servers.	option	-	443								

Parameter	Description	Type	Size	Default
	Option	Description		
	8888	port 8888 for server communication.		
	53	port 53 for server communication.		
	80	port 80 for server communication.		
	443	port 443 for server communication.		
service-account-id	Service account ID.	string	Maximum length: 50	
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266	1
auto-join-forticloud	Automatically connect to and login to FortiCloud.	option	-	disable
	Option	Description		
	enable	Enable automatic connection and login to FortiCloud.		
	disable	Disable automatic connection and login to FortiCloud.		
update-server-location	Location from which to receive FortiGuard updates.	option	-	automatic
	Option	Description		
	automatic	FortiGuard servers chosen based on closest proximity to FortiGate unit.		
	usa	FortiGuard servers in United States.		
	eu	FortiGuard servers in the European Union.		
sandbox-region	FortiCloud Sandbox region.	string	Maximum length: 63	
sandbox-inline-scan	Enable/disable FortiCloud Sandbox inline-scan.	option	-	disable
	Option	Description		
	enable	Enable FortiCloud Sandbox inline scan.		
	disable	Disable FortiCloud Sandbox inline scan.		

Parameter	Description	Type	Size	Default						
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-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.									
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-build-proxy	Enable/disable proxy dictionary rebuild.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable proxy dictionary rebuild.</td></tr><tr><td><i>disable</i></td><td>Disable proxy dictionary rebuild.</td></tr></table>	Option	Description	<i>enable</i>	Enable proxy dictionary rebuild.	<i>disable</i>	Disable proxy dictionary rebuild.			
Option	Description									
<i>enable</i>	Enable proxy dictionary rebuild.									
<i>disable</i>	Disable proxy dictionary rebuild.									
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></table>	Option	Description	<i>enable</i>	Enable persistent connection to receive update notification from FortiGuard.					
Option	Description									
<i>enable</i>	Enable persistent connection to receive update notification from FortiGuard.									

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable persistent connection to receive update notification from FortiGuard.</td></tr></table>	Option	Description	<i>disable</i>	Disable persistent connection to receive update notification from FortiGuard.															
	Option	Description																		
<i>disable</i>	Disable persistent connection to receive update notification from FortiGuard.																			
vdom	FortiGuard Service virtual domain name.	string	Maximum length: 31																	
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	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic patch-level firmware upgrade to latest version from FortiGuard.</td></tr><tr><td><i>disable</i></td><td>Disable automatic patch-level firmware upgrade to latest version from FortiGuard.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic patch-level firmware upgrade to latest version from FortiGuard.	<i>disable</i>	Disable automatic patch-level firmware upgrade to latest version from FortiGuard.													
	Option	Description																		
	<i>enable</i>	Enable automatic patch-level firmware upgrade to latest version from FortiGuard.																		
<i>disable</i>	Disable automatic patch-level firmware upgrade to latest version from FortiGuard.																			
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.																			

Parameter	Description	Type	Size	Default						
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: 0 Maximum value: 14	3						
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: 0 Maximum value: 23	1						
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: 0 Maximum value: 23	4						
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-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Turn off the FortiGuard antispam service.</td></tr><tr><td><i>disable</i></td><td>Allow the FortiGuard antispam service.</td></tr></table>				Option	Description	<i>enable</i>	Turn off the FortiGuard antispam service.	<i>disable</i>	Allow the FortiGuard antispam service.
Option	Description									
<i>enable</i>	Turn off the FortiGuard antispam service.									
<i>disable</i>	Allow the FortiGuard antispam service.									
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><i>enable</i></td><td>Enable FortiGuard antispam request caching.</td></tr></table>				Option	Description	<i>enable</i>	Enable FortiGuard antispam request caching.		
Option	Description									
<i>enable</i>	Enable FortiGuard antispam request caching.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiGuard antispam request caching.</td></tr></table>	Option	Description	<i>disable</i>	Disable FortiGuard antispam request caching.					
Option	Description									
<i>disable</i>	Disable FortiGuard antispam request caching.									
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-cache-mpermille	Maximum permille of FortiProxy memory the antispam cache is allowed to use (1 - 150).	integer	Minimum value: 1 Maximum value: 150	1						
antispam-license	Interval of time between license checks for the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
antispam-expiration	Expiration date of the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	0						
antispam-timeout	Antispam query time out (1 - 30 sec, default = 7).	integer	Minimum value: 1 Maximum value: 30	7						
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Turn off FortiGuard antivirus service.</td></tr><tr><td><i>disable</i></td><td>Allow the FortiGuard antivirus service.</td></tr></table>	Option	Description	<i>enable</i>	Turn off FortiGuard antivirus service.	<i>disable</i>	Allow the FortiGuard antivirus service.			
Option	Description									
<i>enable</i>	Turn off FortiGuard antivirus service.									
<i>disable</i>	Allow the FortiGuard antivirus service.									
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard antivirus caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard antivirus caching.					
Option	Description									
<i>enable</i>	Enable FortiGuard antivirus caching.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiGuard antivirus caching.</td></tr></table>	Option	Description	<i>disable</i>	Disable FortiGuard antivirus caching.					
Option	Description									
<i>disable</i>	Disable FortiGuard antivirus caching.									
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries (300 - 86400 sec, default = 300).	integer	Minimum value: 300 Maximum value: 86400	300						
outbreak-prevention-cache-mpermille	Maximum permille of memory FortiGuard Virus Outbreak Prevention cache can use (1 - 150 permille, default = 1).	integer	Minimum value: 1 Maximum value: 150	1						
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	0						
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out (1 - 30 sec, default = 7).	integer	Minimum value: 1 Maximum value: 30	7						
fnbi-license	License type.	integer	Minimum value: 0 Maximum value: 4294967295	0						
fnbi-expiration	License expiration.	integer	Minimum value: 0 Maximum value: 4294967295	0						
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Turn off the FortiGuard web filtering service.</td></tr><tr><td><i>disable</i></td><td>Allow the FortiGuard web filtering service to operate.</td></tr></table>	Option	Description	<i>enable</i>	Turn off the FortiGuard web filtering service.	<i>disable</i>	Allow the FortiGuard web filtering service to operate.			
Option	Description									
<i>enable</i>	Turn off the FortiGuard web filtering service.									
<i>disable</i>	Allow the FortiGuard web filtering service to operate.									

Parameter	Description	Type	Size	Default
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiGuard web filter caching.		
	<i>disable</i>	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-license	Interval of time between license checks for the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
webfilter-expiration	Expiration date of the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
webfilter-timeout	Web filter query time out (1 - 30 sec, default = 15).	integer	Minimum value: 1 Maximum value: 30	15
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: 1 Maximum value: 65535	53
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
sdns-options	Customization options for the FortiGuard DNS service.	option	-	

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include-question-section</i></td><td>Include DNS question section in the FortiGuard DNS setup message.</td></tr></table>				Option	Description	<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.		
	Option	Description								
<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.									
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	::						
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 Maximum value: 65535	0						
proxy-username	Proxy user name.	string	Maximum length: 64							
proxy-password	Proxy user password.	password	Not Specified							
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						
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
	Option	Description								
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config system fortiguard-log-service

Configuration of FortiCloud log service.

```
config system fortiguard-log-service
    Description: Configuration of FortiCloud log service.
end
```

config system fortiguard-service

Configuration of FortiGuard services.

```
config system fortiguard-service
    Description: Configuration of FortiGuard services.
end
```

config system fortindr

Configure FortiNDR.

```
config system fortindr
    Description: Configure FortiNDR.
    set status [disable|enable]
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config system fortindr

Parameter	Description	Type	Size	Default
status	Enable/disable FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable FortiNDR.		
	<i>enable</i>	Enable FortiNDR.		
source-ip	Source IP address for communications to FortiNDR.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system fortisandbox

Configure FortiSandbox.

```

config system fortisandbox
  Description: Configure FortiSandbox.
  set status [enable|disable]
  set forticloud [enable|disable]
  set inline-scan [enable|disable]
  set server {string}
  set alt-server {string}
  set health-check-interval {integer}
  set source-ip {string}
  set interface-select-method [auto|specify]
  set interface {string}
  set enc-algorithm [default|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set email {string}
end

```

config system fortisandbox

Parameter	Description	Type	Size	Default						
status	Enable/disable FortiSandbox.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiSandbox.</td></tr><tr><td><i>disable</i></td><td>Disable FortiSandbox.</td></tr></table>				Option	Description	<i>enable</i>	Enable FortiSandbox.	<i>disable</i>	Disable FortiSandbox.
	Option	Description								
	<i>enable</i>	Enable FortiSandbox.								
	<i>disable</i>	Disable FortiSandbox.								
forticloud	Enable/disable FortiSandbox Cloud.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable FortiSandbox Cloud.		
	<i>disable</i>	Disable FortiSandbox Cloud.		
inline-scan	Enable/disable FortiSandbox inline scan.	option	-	disable
	Option Description			
	<i>enable</i>	Enable FortiSandbox inline scan.		
	<i>disable</i>	Disable FortiSandbox inline scan.		
server	Server IP address or FQDN of the remote FortiSandbox.	string	Maximum length: 63	
alt-server	Server address of the alternative remote FortiSandbox.	string	Maximum length: 63	
health-check-interval	FortiSandbox failover health check interval in seconds.	integer	Minimum value: 1 Maximum value: 120	5
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option Description			
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	default
	Option Description			
	<i>default</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.		

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
	Option	Description		
	default	Follow system global setting.		
	SSLv3	SSLv3.		
	TLSv1	TLSv1.		
	TLSv1-1	TLSv1.1.		
	TLSv1-2	TLSv1.2.		
	TLSv1-3	TLSv1.3.		
email	Notifier email address.	string	Maximum length: 63	

config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```

config system fsso-polling
  Description: Configure Fortinet Single Sign On (FSSO) server.
  set status [enable|disable]
  set listening-port {integer}
  set authentication [enable|disable]
  set auth-password {password}
end

```

config system fsso-polling

Parameter	Description	Type	Size	Default						
status	Enable/disable FSSO Polling Mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FSSO Polling Mode.</td></tr><tr><td><i>disable</i></td><td>Disable FSSO Polling Mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable FSSO Polling Mode.	<i>disable</i>	Disable FSSO Polling Mode.			
Option	Description									
<i>enable</i>	Enable FSSO Polling Mode.									
<i>disable</i>	Disable FSSO Polling Mode.									

Parameter	Description	Type	Size	Default						
listening-port	Listening port to accept clients (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	8000						
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FSSO Agent Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable FSSO Agent Authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable FSSO Agent Authentication.	<i>disable</i>	Disable FSSO Agent Authentication.
	Option	Description								
	<i>enable</i>	Enable FSSO Agent Authentication.								
<i>disable</i>	Disable FSSO Agent Authentication.									
auth-password	Password to connect to FSSO Agent.	password	Not Specified							

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-port {integer}
  set server-cert {string}
  set server-ip {ipv4-address}
  set server {string}
  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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable communication to the proxy server in FortiGuard configuration.</td></tr><tr><td><i>disable</i></td><td>Disable communication to the proxy server in FortiGuard configuration.</td></tr></table>				Option	Description	<i>enable</i>	Enable communication to the proxy server in FortiGuard configuration.	<i>disable</i>	Disable communication to the proxy server in FortiGuard configuration.
Option	Description									
<i>enable</i>	Enable communication to the proxy server in FortiGuard configuration.									
<i>disable</i>	Disable communication to the proxy server in FortiGuard configuration.									

Parameter	Description	Type	Size	Default						
server-port	Port to communicate with FortiToken Mobile push services server (1 - 65535, default = 4433).	integer	Minimum value: 1 Maximum value: 65535	4433						
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	IPv4 address or domain name of FortiToken Mobile push services server.	string	Maximum length: 127							
status	Enable/disable the use of FortiToken Mobile push services.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiToken Mobile push services.</td></tr><tr><td><i>disable</i></td><td>Disable FortiToken Mobile push services.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiToken Mobile push services.	<i>disable</i>	Disable FortiToken Mobile push services.			
Option	Description									
<i>enable</i>	Enable FortiToken Mobile push services.									
<i>disable</i>	Disable FortiToken Mobile push services.									

config system geoip-country

Define geoip country name-ID table.

```
config system geoip-country
    Description: Define geoip country name-ID table.
    edit <id>
        set name {string}
    next
end
```

config system geoip-country

Parameter	Description	Type	Size	Default
id	Country ID.	string	Maximum length: 2	
name	Country name.	string	Maximum length: 63	

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 description {string}
        set country-id {string}
        config ip-range
            Description: Table of IP ranges assigned to country.
            edit <id>
                set start-ip {ipv4-address}
                set end-ip {ipv4-address}
            next
        end
        config ip6-range
            Description: Table of IPv6 ranges assigned to country.
            edit <id>
                set start-ip {ipv6-address}
                set end-ip {ipv6-address}
            next
        end
    next
end

```

config system geoip-override

Parameter	Description	Type	Size	Default
name	Location name.	string	Maximum length: 63	
description	Description.	string	Maximum length: 127	
country-id	Two character Country ID code.	string	Maximum length: 2	

config ip-range

Parameter	Description	Type	Size	Default
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
end-ip	Ending 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
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	::
end-ip	Ending 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 language [english|french|...]
  set gui-allow-incompatible-fabric-ftg [enable|disable]
  set gui-ipv6 [enable|disable]
  set gui-replacement-message-groups [enable|disable]
  set gui-local-out [enable|disable]
  set gui-certificates [enable|disable]
  set gui-custom-language [enable|disable]
  set gui-app-detection-sdwan [enable|disable]
  set gui-display-hostname [enable|disable]
  set gui-fortigate-cloud-sandbox [enable|disable]
  set gui-firmware-upgrade-warning [enable|disable]
  set gui-forticare-registration-setup-warning [enable|disable]
  set gui-auto-upgrade-setup-warning [enable|disable]
  set gui-workflow-management [enable|disable]
  set gui-cdn-usage [enable|disable]
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admin-https-ssl-ciphersuites {option1}, {option2}, ...
  set admin-https-ssl-banned-ciphers {option1}, {option2}, ...
  set admin-timeout {integer}
  set admin-console-timeout {integer}
  set ssd-trim-freq [never|hourly|...]
  set ssd-trim-hour {integer}
  set ssd-trim-min {integer}
  set ssd-trim-weekday [sunday|monday|...]
  set ssd-trim-date {integer}
  set admin-concurrent [enable|disable]
```

```
set admin-lockout-threshold {integer}
set admin-lockout-duration {integer}
set refresh {integer}
set interval {integer}
set failtime {integer}
set purdue-level [1|1.5|...]
set daily-restart [enable|disable]
set restart-time {user}
set wad-restart-mode [none|time|...]
set wad-restart-start-time {user}
set wad-restart-end-time {user}
set radius-port {integer}
set speedtestd-server-port {integer}
set speedtestd-ctrl-port {integer}
set admin-login-max {integer}
set remoteauthtimeout {integer}
set ldapconntimeout {integer}
set batch-cmdb [enable|disable]
set multi-factor-authentication [optional|mandatory]
set ssl-min-proto-version [SSLv3|TLSv1|...]
set autorun-log-fsck [enable|disable]
set timezone {string}
set traffic-priority [tos|dscp]
set traffic-priority-level [low|medium|...]
set quic-congestion-control-algo [cubic|bbr|...]
set quic-max-datagram-size {integer}
set quic-udp-payload-size-shaping-per-cid [enable|disable]
set quic-ack-threshold {integer}
set quic-pmtud [enable|disable]
set quic-tls-handshake-timeout {integer}
set anti-replay [disable|loose|...]
set pmtu-discovery [enable|disable]
set revision-image-auto-backup [enable|disable]
set revision-backup-on-logout [enable|disable]
set hostname {string}
set alias {string}
set strong-crypto [enable|disable]
set ssl-static-key-ciphers [enable|disable]
set snat-route-change [enable|disable]
set speedtest-server [enable|disable]
set cli-audit-log [enable|disable]
set dh-params [1024|1536|...]
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set tcp-option [enable|disable]
set lldp-transmission [enable|disable]
set lldp-reception [enable|disable]
set proxy-auth-timeout {integer}
set proxy-keep-alive-mode [session|traffic|...]
set proxy-re-authentication-time {integer}
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
```

```
set proxy-auth-machine-timeout {integer}
set proxy-resource-mode [enable|disable]
set proxy-cert-use-mgmt-vdom [enable|disable]
set update-tls-finger-print [enable|disable]
set sys-perf-log-interval {integer}
set check-protocol-header [loose|strict]
set vip-arp-range [unlimited|restricted]
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-timewait-timer {integer}
set tcp-rst-timer {integer}
set udp-idle-timer {integer}
set block-session-timer {integer}
set ip-src-port-range {user}
set pre-login-banner [enable|disable]
set post-login-banner [disable|enable]
set tftp [enable|disable]
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set kernel-panic-timeout {integer}
set kernel-panic-debug [enable|disable]
set kernel-panic-on-warn [enable|disable]
set memory-use-threshold-extreme {integer}
set memory-use-threshold-red {integer}
set memory-use-threshold-green {integer}
set ip-fragment-mem-thresholds {integer}
set cpu-use-threshold {integer}
set log-single-cpu-high [enable|disable]
set check-reset-range [strict|disable]
set admin-port {integer}
set admin-sport {integer}
set admin-host {string}
set admin-https-redirect [enable|disable]
set admin-hsts-max-age {integer}
set admin-ssh-password [enable|disable]
set admin-restrict-local [enable|disable]
set admin-ssh-port {integer}
set admin-ssh-grace-time {integer}
set admin-ssh-v1 [enable|disable]
set admin-telnet [enable|disable]
set admin-telnet-port {integer}
set admin-forticloud-sso-login [enable|disable]
set admin-forticloud-sso-default-profile {string}
set default-service-source-port {user}
set admin-server-cert {string}
set admin-https-pki-required [enable|disable]
set auth-http-port {integer}
set auth-https-port {integer}
set auth-ike-saml-port {integer}
set auth-keepalive [enable|disable]
set policy-auth-concurrent {integer}
set auth-session-limit [block-new|logout-inactive]
```

```

set auth-cert {string}
set clt-cert-req [enable|disable]
set fortiservice-port {integer}
set cfg-save [automatic|manual|...]
set cfg-revert-timeout {integer}
set reboot-upon-config-restore [enable|disable]
set admin-scp [enable|disable]
set security-rating-run-on-schedule [enable|disable]
set fortiextender-data-port {integer}
set fortiextender [disable|enable]
set extender-controller-reserved-network {ipv4-classnet-host}
set fortiextender-discovery-lockdown [disable|enable]
set fortiextender-provision-on-authorization [enable|disable]
set dnsproxy-worker-count {integer}
set url-filter-count {integer}
set proxy-worker-count {integer}
set scanunit-count {integer}
set fgd-alert-subscription {option1}, {option2}, ...
set ipv6-accept-dad {integer}
set ipv6-allow-multicast-probe [enable|disable]
set ipv6-allow-local-in-silent-drop [enable|disable]
set csr-ca-attribute [enable|disable]
set wimax-4g-usb [enable|disable]
set cert-chain-max {integer}
set two-factor-ftk-expiry {integer}
set two-factor-email-expiry {integer}
set two-factor-sms-expiry {integer}
set two-factor-fac-expiry {integer}
set two-factor-ftm-expiry {integer}
set max-img-cache-size {integer}
set img-cache-mode [stop|rolling]
set per-user-bal [enable|disable]
set wad-worker-count {integer}
set wad-csvc-cs-count {integer}
set wad-csvc-db-count {integer}
set http-view [enable|disable]
set wad-source-affinity [disable|enable]
set wad-memory-change-granularity {integer}
set login-timestamp [enable|disable]
set miglogd-children {integer}
set special-file-23-support [disable|enable]
set log-uuid-address [enable|disable]
set log-ssl-connection [enable|disable]
set gui-rest-api-cache [enable|disable]
set rest-api-key-url-query [enable|disable]
set gui-cdn-domain-override {string}
set arp-max-entry {integer}
set ha-affinity {string}
set bfd-affinity {string}
set cmdbsvr-affinity {string}
set av-affinity {string}
set wad-affinity {string}

```

```

set ips-affinity {string}
set miglog-affinity {string}
set syslog-affinity {string}
set url-filter-affinity {string}
set ndp-max-entry {integer}
set br-fdb-max-entry {integer}
set max-route-cache-size {integer}
set ipsec-round-robin [enable|disable]
set device-idle-timeout {integer}
set user-device-store-max-devices {integer}
set user-device-store-max-users {integer}
set user-device-store-max-unified-mem {integer}
set gui-device-latitude {string}
set gui-device-longitude {string}
set v-tpm [disable|enable]
set private-data-encryption [disable|enable]
set auto-auth-extension-device [enable|disable]
set gui-theme [jade|neutrino|...]
set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
set gui-date-time-source [system|browser]
set igmp-state-limit {integer}
set cloud-communication [enable|disable]
set ipsec-ha-seqjump-rate {integer}
set fortitoken-cloud [enable|disable]
set fortitoken-cloud-push-status [enable|disable]
set fortitoken-cloud-sync-interval {integer}
set faz-disk-buffer-size {integer}
set irq-time-accounting [auto|force]
set management-ip {string}
set management-port {integer}
set management-port-use-admin-sport [enable|disable]
set forticonverter-integration [enable|disable]
set forticonverter-config-upload [once|disable]
set internet-service-database [mini|standard|...]
set internet-service-download-list <id1>, <id2>, ...
set early-tcp-npu-session [enable|disable]
set interface-subnet-usage [disable|enable]
set sflowd-max-children-num {integer}
set fortigslb-integration [disable|enable]
set license-overlimit [bypass|block]
set max-session-per-user {integer}
set conntrack {integer}
set established-timeout {integer}
set time-wait-timeout {integer}
set fin-wait-timeout {integer}
set close-wait-timeout {integer}
set syn-sent-timeout {integer}
set syn-recv-timeout {integer}
set last-ack-timeout {integer}
set udp-timeout {integer}
set udp-stream-timeout {integer}
set username-case-sensitivity [enable|disable]

```

```

set tcp-random-source-port [enable|disable]
end

```

config system global

Parameter	Description	Type	Size	Default
language	GUI display language.	option	-	english
	Option	Description		
	english	English.		
	french	French.		
	spanish	Spanish.		
	portuguese	Portuguese.		
	japanese	Japanese.		
	trach	Traditional Chinese.		
	simch	Simplified Chinese.		
korean	Korean.			
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		
	enable	Display the feature in GUI.		
	disable	Do not display the feature in GUI.		
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	disable
	Option	Description		
	enable	Display the feature in GUI.		
	disable	Do not display the feature in GUI.		
gui-replacement-message-groups	Enable/disable replacement message groups 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-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-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-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-display-hostname	Enable/disable displaying the FortiProxy's hostname on the GUI login page.	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-fortigate-cloud-sandbox	Enable/disable displaying FortiProxy Cloud Sandbox 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-firmware-upgrade-warning	Enable/disable the firmware upgrade warning on 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-forticare-registration-setup-warning	Enable/disable the FortiCare registration setup warning on 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-auto-upgrade-setup-warning	Enable/disable the automatic patch upgrade setup prompt on 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-workflow-management	Enable/disable Workflow management features 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-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.		
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-	tlsv1-2 tlsv1-3
	Option	Description		
	<i>tlsv1-1</i>	TLS 1.1.		
	<i>tlsv1-2</i>	TLS 1.2.		
	<i>tlsv1-3</i>	TLS 1.3.		
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		
	<i>TLS-AES-128-GCM-SHA256</i>	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.		
	<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.		

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></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-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.																																	
	Option	Description																																				
<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.																																					
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><i>RSA</i></td><td>Ban the use of cipher suites using RSA key.</td></tr><tr><td><i>DHE</i></td><td>Ban the use of cipher suites using authenticated ephemeral DH key agreement.</td></tr><tr><td><i>ECDHE</i></td><td>Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.</td></tr><tr><td><i>DSS</i></td><td>Ban the use of cipher suites using DSS authentication.</td></tr><tr><td><i>ECDSA</i></td><td>Ban the use of cipher suites using ECDSA authentication.</td></tr><tr><td><i>AES</i></td><td>Ban the use of cipher suites using either 128 or 256 bit AES.</td></tr><tr><td><i>AESGCM</i></td><td>Ban the use of cipher suites using AES in Galois Counter Mode (GCM).</td></tr><tr><td><i>CAMELLIA</i></td><td>Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.</td></tr><tr><td><i>3DES</i></td><td>Ban the use of cipher suites using triple DES.</td></tr><tr><td><i>SHA1</i></td><td>Ban the use of cipher suites using HMAC-SHA1.</td></tr><tr><td><i>SHA256</i></td><td>Ban the use of cipher suites using HMAC-SHA256.</td></tr><tr><td><i>SHA384</i></td><td>Ban the use of cipher suites using HMAC-SHA384.</td></tr><tr><td><i>STATIC</i></td><td>Ban the use of cipher suites using static keys.</td></tr><tr><td><i>CHACHA20</i></td><td>Ban the use of cipher suites using ChaCha20.</td></tr><tr><td><i>ARIA</i></td><td>Ban the use of cipher suites using ARIA.</td></tr><tr><td><i>AESCCM</i></td><td>Ban the use of cipher suites using AESCCM.</td></tr></table>	Option	Description	<i>RSA</i>	Ban the use of cipher suites using RSA key.	<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.	<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.	<i>DSS</i>	Ban the use of cipher suites using DSS authentication.	<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.	<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.	<i>AESGCM</i>	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).	<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.	<i>3DES</i>	Ban the use of cipher suites using triple DES.	<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.	<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.	<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.	<i>STATIC</i>	Ban the use of cipher suites using static keys.	<i>CHACHA20</i>	Ban the use of cipher suites using ChaCha20.	<i>ARIA</i>	Ban the use of cipher suites using ARIA.	<i>AESCCM</i>	Ban the use of cipher suites using AESCCM.			
	Option	Description																																				
	<i>RSA</i>	Ban the use of cipher suites using RSA key.																																				
	<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.																																				
	<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.																																				
	<i>DSS</i>	Ban the use of cipher suites using DSS authentication.																																				
	<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.																																				
	<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.																																				
	<i>AESGCM</i>	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).																																				
	<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.																																				
	<i>3DES</i>	Ban the use of cipher suites using triple DES.																																				
	<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.																																				
	<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.																																				
	<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.																																				
	<i>STATIC</i>	Ban the use of cipher suites using static keys.																																				
	<i>CHACHA20</i>	Ban the use of cipher suites using ChaCha20.																																				
<i>ARIA</i>	Ban the use of cipher suites using ARIA.																																					
<i>AESCCM</i>	Ban the use of cipher suites using AESCCM.																																					

Parameter	Description	Type	Size	Default												
admin-timeout	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												
admin-console-timeout	Console login timeout that overrides the admin timeout value (15 - 300 seconds, default = 0, which disables the timeout).	integer	Minimum value: 15 Maximum value: 300	0												
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><i>never</i></td><td>Never Run SSD Trim.</td></tr><tr><td><i>hourly</i></td><td>Run SSD Trim Hourly.</td></tr><tr><td><i>daily</i></td><td>Run SSD Trim Daily.</td></tr><tr><td><i>weekly</i></td><td>Run SSD Trim Weekly.</td></tr><tr><td><i>monthly</i></td><td>Run SSD Trim Monthly.</td></tr></table>	Option	Description	<i>never</i>	Never Run SSD Trim.	<i>hourly</i>	Run SSD Trim Hourly.	<i>daily</i>	Run SSD Trim Daily.	<i>weekly</i>	Run SSD Trim Weekly.	<i>monthly</i>	Run SSD Trim Monthly.			
Option	Description															
<i>never</i>	Never Run SSD Trim.															
<i>hourly</i>	Run SSD Trim Hourly.															
<i>daily</i>	Run SSD Trim Daily.															
<i>weekly</i>	Run SSD Trim Weekly.															
<i>monthly</i>	Run SSD Trim Monthly.															
ssd-trim-hour	Hour of the day on which to run SSD Trim (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23	1												
ssd-trim-min	Minute of the hour on which to run SSD Trim (0 - 59, 60 for random).	integer	Minimum value: 0 Maximum value: 60	60												
ssd-trim-weekday	Day of week to run SSD Trim.	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></table>	Option	Description	<i>sunday</i>	Sunday	<i>monday</i>	Monday	<i>tuesday</i>	Tuesday							
Option	Description															
<i>sunday</i>	Sunday															
<i>monday</i>	Monday															
<i>tuesday</i>	Tuesday															

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></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	wednesday	Wednesday	thursday	Thursday	friday	Friday	saturday	Saturday			
	Option	Description												
	wednesday	Wednesday												
	thursday	Thursday												
	friday	Friday												
saturday	Saturday													
ssd-trim-date	Date within a month to run ssd trim.	integer	Minimum value: 1 Maximum value: 31	1										
admin-concurrent	Enable/disable concurrent administrator logins. Use policy-auth-concurrent for firewall authenticated users.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable admin concurrent login.</td></tr><tr><td>disable</td><td>Disable admin concurrent login.</td></tr></table>	Option	Description	enable	Enable admin concurrent login.	disable	Disable admin concurrent login.							
	Option	Description												
	enable	Enable admin concurrent login.												
disable	Disable admin concurrent login.													
admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 1 Maximum value: 10	3										
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: 1 Maximum value: 2147483647	60										
refresh	Statistics refresh interval second(s) in GUI.	integer	Minimum value: 0 Maximum value: 4294967295	0										
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295	5										

Parameter	Description	Type	Size	Default																				
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295	5																				
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																							
daily-restart	Enable/disable daily restart of FortiProxy unit. Use the restart-time option to set the time of day for the restart.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable daily reboot of the FortiProxy.</td></tr><tr><td>disable</td><td>Disable daily reboot of the FortiProxy.</td></tr></table>	Option	Description	enable	Enable daily reboot of the FortiProxy.	disable	Disable daily reboot of the FortiProxy.																	
	Option	Description																						
	enable	Enable daily reboot of the FortiProxy.																						
disable	Disable daily reboot of the FortiProxy.																							
restart-time	Daily restart time (hh:mm).	user	Not Specified																					
wad-restart-mode	WAD worker restart mode (default = none).	option	-	none																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Disable restart of WAD workers.</td></tr><tr><td>time</td><td>Enable daily restart of WAD workers.</td></tr><tr><td>memory</td><td>Enable restart of WAD workers based on memory usage.</td></tr></table>	Option	Description	none	Disable restart of WAD workers.	time	Enable daily restart of WAD workers.	memory	Enable restart of WAD workers based on memory usage.															
	Option	Description																						
	none	Disable restart of WAD workers.																						
	time	Enable daily restart of WAD workers.																						
memory	Enable restart of WAD workers based on memory usage.																							

Parameter	Description	Type	Size	Default
wad-restart-start-time	WAD workers daily restart time (hh:mm).	user	Not Specified	
wad-restart-end-time	WAD workers daily restart end time (hh:mm).	user	Not Specified	
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812
speedtestd-server-port	Speedtest server port number.	integer	Minimum value: 1 Maximum value: 65535	5201
speedtestd-ctrl-port	Speedtest server controller port number.	integer	Minimum value: 1 Maximum value: 65535	5200
admin-login-max	Maximum number of administrators who can be logged in at the same time (1 - 100, default = 100).	integer	Minimum value: 1 Maximum value: 100	100
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: 1 Maximum value: 300	5
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds (1 - 300000, default 500).	integer	Minimum value: 1 Maximum value: 300000	500
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
		Option	Description	
		<i>enable</i>	Enable batch mode to execute in CMDB server.	
		<i>disable</i>	Disable batch mode to execute in CMDB server.	

Parameter	Description	Type	Size	Default												
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.															
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><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>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>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.															
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><i>enable</i></td><td>Enable automatic log partition check after ungraceful shutdown.</td></tr><tr><td><i>disable</i></td><td>Disable automatic log partition check after ungraceful shutdown.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.	<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.									
Option	Description															
<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.															
<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.															
timezone	Timezone database name. Enter ? to view the list of timezone.	string	Maximum length: 63													
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos												

Parameter	Description	Type	Size	Default
	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.		
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-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.		
quic-ack-threshold	Maximum number of unacknowledged packets before sending ACK (2 - 5, default = 3).	integer	Minimum value: 2 Maximum value: 5	3

Parameter	Description	Type	Size	Default								
quic-pmtud	Enable/disable path MTU discovery (default = enable).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable path MTU discovery.</td></tr><tr><td><i>disable</i></td><td>Disable path MTU discovery.</td></tr></table>	Option	Description	<i>enable</i>	Enable path MTU discovery.	<i>disable</i>	Disable path MTU discovery.					
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								
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><i>disable</i></td><td>Disable anti-replay check.</td></tr><tr><td><i>loose</i></td><td>Loose anti-replay check.</td></tr><tr><td><i>strict</i></td><td>Strict anti-replay check.</td></tr></table>	Option	Description	<i>disable</i>	Disable anti-replay check.	<i>loose</i>	Loose anti-replay check.	<i>strict</i>	Strict anti-replay check.			
Option	Description											
<i>disable</i>	Disable anti-replay check.											
<i>loose</i>	Loose anti-replay check.											
<i>strict</i>	Strict anti-replay check.											
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable path MTU discovery.</td></tr><tr><td><i>disable</i></td><td>Disable path MTU discovery.</td></tr></table>	Option	Description	<i>enable</i>	Enable path MTU discovery.	<i>disable</i>	Disable path MTU discovery.					
Option	Description											
<i>enable</i>	Enable path MTU discovery.											
<i>disable</i>	Disable path MTU discovery.											
revision-image-auto-backup	Enable/disable back-up of the latest image revision after the firmware is upgraded.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable revision image backup automatically when upgrading image.</td></tr><tr><td><i>disable</i></td><td>Disable revision image backup automatically when upgrading image.</td></tr></table>	Option	Description	<i>enable</i>	Enable revision image backup automatically when upgrading image.	<i>disable</i>	Disable revision image backup automatically when upgrading image.					
Option	Description											
<i>enable</i>	Enable revision image backup automatically when upgrading image.											
<i>disable</i>	Disable revision image backup automatically when upgrading image.											

Parameter	Description	Type	Size	Default
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
	Option Description			
	enable Enable revision config backup automatically when logout.			
	disable Disable revision config backup automatically when logout.			
hostname	FortiProxy unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35	
alias	Alias for your FortiProxy unit.	string	Maximum length: 35	
strong-crypto	Enable to use strong encryption and only allow strong ciphers and digest for HTTPS/SSH/TLS/SSL functions.	option	-	enable
	Option Description			
	enable Enable strong crypto for HTTPS/SSH/TLS/SSL.			
	disable Disable strong crypto for HTTPS/SSH/TLS/SSL.			
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
	Option Description			
	enable Enable static key ciphers in SSL/TLS connections.			
	disable Disable static key ciphers in SSL/TLS connections.			
snat-route-change	Enable/disable the ability to change the source NAT route.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable SNAT route change.		
	<i>disable</i>	Disable SNAT route change.		
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.		
cli-audit-log	Enable/disable CLI audit log.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable CLI audit log.		
	<i>disable</i>	Disable CLI audit log.		
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048
	Option	Description		
	<i>1024</i>	1024 bits.		
	<i>1536</i>	1536 bits.		
	<i>2048</i>	2048 bits.		
	<i>3072</i>	3072 bits.		
	<i>4096</i>	4096 bits.		
	<i>6144</i>	6144 bits.		
	<i>8192</i>	8192 bits.		
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

Parameter	Description	Type	Size	Default
	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: 1 Maximum value: 1440	60
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TCP option.		
	<i>disable</i>	Disable TCP option.		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).		
	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).		
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).		
	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).		
proxy-auth-timeout	Authentication timeout in minutes for authenticated users (1 - 10000 min, default = 10).	integer	Minimum value: 1 Maximum value: 10000	10

Parameter	Description	Type	Size	Default
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
	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.		
	<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: 1 Maximum value: 86400	30
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
	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-machine-timeout	Machine account timeout in seconds for authenticated machines (5 - 30 seconds, default=15s).	integer	Minimum value: 5 Maximum value: 30	15

Parameter	Description	Type	Size	Default						
proxy-resource-mode	Enable/disable use of the maximum memory usage on the FortiProxy 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-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.									
update-tls-finger-print	Enable/disable update TLS fingerprint when deep-inspection is enabled.	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.									
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						
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></table>	Option	Description	<i>loose</i>	Check protocol header loosely.					
Option	Description									
<i>loose</i>	Check protocol header loosely.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Check protocol header strictly.</td></tr></table>	Option	Description	<i>strict</i>	Check protocol header strictly.					
	Option	Description								
	<i>strict</i>	Check protocol header strictly.								
vip-arp-range	Controls the number of ARPs that the FortiProxy sends for a Virtual IP (VIP) address range.	option	-	restricted						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unlimited</i></td><td>Send ARPs for all addresses in VIP range.</td></tr><tr><td><i>restricted</i></td><td>Send ARPs for the first 8192 addresses in VIP range.</td></tr></table>	Option	Description	<i>unlimited</i>	Send ARPs for all addresses in VIP range.	<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.			
	Option	Description								
	<i>unlimited</i>	Send ARPs for all addresses in VIP range.								
<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.									
tcp-halfclose-timer	Number of seconds the FortiProxy 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						
tcp-halfopen-timer	Number of seconds the FortiProxy 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-timewait-timer	Length of the TCP TIME-WAIT state in seconds (1 - 300 sec, default = 1).	integer	Minimum value: 0 Maximum value: 300	1						
tcp-rst-timer	Length of the TCP CLOSE state in seconds (5 - 300 sec, default = 5).	integer	Minimum value: 5 Maximum value: 300	5						
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						

Parameter	Description	Type	Size	Default						
block-session-timer	Duration in seconds for blocked sessions (1 - 300 sec (5 minutes), default = 30).	integer	Minimum value: 1 Maximum value: 300	30						
ip-src-port-range	IP source port range used for traffic originating from the FortiProxy unit.	user	Not Specified	1024-65001						
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pre-login banner.</td></tr><tr><td><i>disable</i></td><td>Disable pre-login banner.</td></tr></table>	Option	Description	<i>enable</i>	Enable pre-login banner.	<i>disable</i>	Disable pre-login banner.			
Option	Description									
<i>enable</i>	Enable pre-login banner.									
<i>disable</i>	Disable pre-login banner.									
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable post-login banner.</td></tr><tr><td><i>enable</i></td><td>Enable post-login banner.</td></tr></table>	Option	Description	<i>disable</i>	Disable post-login banner.	<i>enable</i>	Enable post-login banner.			
Option	Description									
<i>disable</i>	Disable post-login banner.									
<i>enable</i>	Enable post-login banner.									
tftp	Enable/disable TFTP.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TFTP.</td></tr><tr><td><i>disable</i></td><td>Disable TFTP.</td></tr></table>	Option	Description	<i>enable</i>	Enable TFTP.	<i>disable</i>	Disable TFTP.			
Option	Description									
<i>enable</i>	Enable TFTP.									
<i>disable</i>	Disable TFTP.									
av-failopen	Set the action to take if the FortiProxy is running low on memory or the proxy connection limit has been reached.	option	-	pass						

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>enable</i>	Enable AV fail open session option.		
	<i>disable</i>	Disable AV fail open session option.		
kernel-panic-timeout	Reboot timeout after kernel panic in seconds. Value of 0 means do not reboot.	integer	Minimum value: 0 Maximum value: 3600	5
kernel-panic-debug	Enable/disable kernel panic debug messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable kernel panic debug messages.		
	<i>disable</i>	Disable kernel panic debug messages.		
kernel-panic-on-warn	Enable/disable kernel panic and reboot on kernel warning.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable panic and reboot on kernel warning.		
	<i>disable</i>	Disable panic and reboot on kernel warning.		

Parameter	Description	Type	Size	Default						
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 Maximum value: 97	95						
memory-use-threshold-red	Threshold at which memory usage forces the FortiProxy to enter conserve mode (% of total RAM, default = 88).	integer	Minimum value: 70 Maximum value: 97	88						
memory-use-threshold-green	Threshold at which memory usage forces the FortiProxy to exit conserve mode (% of total RAM, default = 82).	integer	Minimum value: 70 Maximum value: 97	82						
ip-fragment-mem-thresholds	Maximum memory (MB) used to reassemble IPv4/IPv6 fragments.	integer	Minimum value: 32 Maximum value: 2047	32						
cpu-use-threshold	Threshold at which CPU usage is reported (% of total CPU, default = 90).	integer	Minimum value: 50 Maximum value: 99	90						
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.									
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.									

Parameter	Description	Type	Size	Default						
admin-port	Administrative access port for HTTP. (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535	80						
admin-sport	Administrative access port for HTTPS. (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535	443						
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-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirecting HTTP administration access to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirecting HTTP administration access to HTTPS.</td></tr></table>				Option	Description	<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.	<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.
Option	Description									
<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.									
<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.									
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						
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-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running (default = disable).	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable local admin authentication restriction.		
	<i>disable</i>	Disable local admin authentication restriction.		
admin-ssh-port	Administrative access port for SSH. (1 - 65535, default = 22).	integer	Minimum value: 1 Maximum value: 65535	22
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiProxy unit and authenticating (10 - 3600 sec (1 hour), default 120).	integer	Minimum value: 10 Maximum value: 3600	120
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable
	Option Description			
	<i>enable</i>	Enable SSH v1 compatibility.		
	<i>disable</i>	Disable SSH v1 compatibility.		
admin-telnet	Enable/disable TELNET service.	option	-	enable
	Option Description			
	<i>enable</i>	Enable TELNET service.		
	<i>disable</i>	Disable TELNET service.		
admin-telnet-port	Administrative access port for TELNET. (1 - 65535, default = 23).	integer	Minimum value: 1 Maximum value: 65535	23
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-forticloud-sso-default-profile	Override access profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
default-service-source-port	Default service source port range (default = 1 - 65535).	user	Not Specified	
admin-server-cert	Server certificate that the FortiProxy uses for HTTPS administrative connections.	string	Maximum length: 35	Fortinet_GUI_Server
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
	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.		
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
	Option		Description	
	enable	Enable use of keep alive to extend authentication.		
	disable	Disable use of keep alive to extend authentication.		

Parameter	Description	Type	Size	Default								
policy-auth-concurrent	Number of concurrent firewall use logins from the same user (1 - 100, default = 0 means no limit).	integer	Minimum value: 0 Maximum value: 100	0								
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><i>block-new</i></td><td>Block new user authentication attempts.</td></tr><tr><td><i>logout-inactive</i></td><td>Logout the most inactive user authenticated sessions.</td></tr></table>	Option	Description	<i>block-new</i>	Block new user authentication attempts.	<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.					
Option	Description											
<i>block-new</i>	Block new user authentication attempts.											
<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.											
auth-cert	Server certificate that the FortiProxy uses for HTTPS firewall authentication connections.	string	Maximum length: 35	Fortinet_Factory								
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable require client certificate for GUI login.</td></tr><tr><td><i>disable</i></td><td>Disable require client certificate for GUI login.</td></tr></table>	Option	Description	<i>enable</i>	Enable require client certificate for GUI login.	<i>disable</i>	Disable require client certificate for GUI login.					
Option	Description											
<i>enable</i>	Enable require client certificate for GUI login.											
<i>disable</i>	Disable require client certificate for GUI login.											
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								
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.											

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						
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reboot of system upon restoring configuration.</td></tr><tr><td>disable</td><td>Disable reboot of system upon restoring configuration.</td></tr></table>	Option	Description	enable	Enable reboot of system upon restoring configuration.	disable	Disable reboot of system upon restoring configuration.			
Option	Description									
enable	Enable reboot of system upon restoring configuration.									
disable	Disable reboot of system upon restoring configuration.									
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><tr><td>disable</td><td>Disable 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.	disable	Disable 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.									
disable	Disable SCP support for system configuration backup, restore, and firmware file upload.									
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable scheduled runs of Security Rating.</td></tr><tr><td>disable</td><td>Disable scheduled runs of Security Rating.</td></tr></table>	Option	Description	enable	Enable scheduled runs of Security Rating.	disable	Disable scheduled runs of Security Rating.			
Option	Description									
enable	Enable scheduled runs of Security Rating.									
disable	Disable scheduled runs of Security Rating.									
fortiextender-data-port	FortiExtender data port (1024 - 49150, default = 25246).	integer	Minimum value: 1024 Maximum value: 49150	25246						
fortiextender	Enable/disable FortiExtender.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable FortiExtender controller.</td></tr><tr><td>enable</td><td>Enable FortiExtender controller.</td></tr></table>	Option	Description	disable	Disable FortiExtender controller.	enable	Enable FortiExtender controller.			
Option	Description									
disable	Disable FortiExtender controller.									
enable	Enable FortiExtender controller.									

Parameter	Description	Type	Size	Default						
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						
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.									
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: 255	1						
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 10	1						
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 255	0						

Parameter	Description	Type	Size	Default														
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiProxy units with multiple CPUs.	integer	Minimum value: 1 Maximum value: 255	0														
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-															
	<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.																	
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2	1														
ipv6-allow-multicast-probe	Enable/disable IPv6 address probe through Multicast.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable probing of IPv6 address space through Multicast.</td></tr><tr><td><i>disable</i></td><td>Disable probing of IPv6 address space through Multicast.</td></tr></table>	Option	Description	<i>enable</i>	Enable probing of IPv6 address space through Multicast.	<i>disable</i>	Disable probing of IPv6 address space through Multicast.											
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-local-in-silent-drop	Enable/disable silent drop of IPv6 local-in traffic.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable silent drop of IPv6 local-in traffic.</td></tr><tr><td><i>disable</i></td><td>Disable silent drop of IPv6 local-in traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable silent drop of IPv6 local-in traffic.	<i>disable</i>	Disable silent drop of IPv6 local-in traffic.											
Option	Description																	
<i>enable</i>	Enable silent drop of IPv6 local-in traffic.																	
<i>disable</i>	Disable silent drop of IPv6 local-in traffic.																	

Parameter	Description	Type	Size	Default						
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable CA attribute in CSR.</td></tr><tr><td><i>disable</i></td><td>Disable CA attribute in CSR.</td></tr></table>	Option	Description	<i>enable</i>	Enable CA attribute in CSR.	<i>disable</i>	Disable CA attribute in CSR.			
Option	Description									
<i>enable</i>	Enable CA attribute in CSR.									
<i>disable</i>	Disable CA attribute in CSR.									
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiMax 4G.</td></tr><tr><td><i>disable</i></td><td>Disable WiMax 4G.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiMax 4G.	<i>disable</i>	Disable WiMax 4G.			
Option	Description									
<i>enable</i>	Enable WiMax 4G.									
<i>disable</i>	Disable WiMax 4G.									
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8						
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-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-sms-expiry	SMS-based two-factor authentication session timeout (30 - 300 sec, 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						

Parameter	Description	Type	Size	Default
two-factor-ftm-expiry	FortiToken Mobile session timeout (1 - 168 hours (7 days), default = 72).	integer	Minimum value: 1 Maximum value: 168	72
max-img-cache-size	Maximum space (MB) can be used by image-analyzer to store blocked images into ram disk.	integer	Minimum value: 30 Maximum value: 300	60
img-cache-mode	Select image cache mode for image-analyzer (default = rolling)	option	-	rolling
	Option		Description	
	<i>stop</i>		Stop caching blocked images into ram disk when limit reaches.	
	<i>rolling</i>		Evict old cached images when limit reaches.	
per-user-bal	Enable/disable per-user block/allow list filter.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable per-user block/allow list filter.	
	<i>disable</i>		Disable per-user block/allow list filter.	
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 Maximum value: 255	0
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1	1
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
http-view	Enable/disable logging and viewing of HTTP/S cache traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging and viewing of HTTP/S cache traffic.		
	<i>disable</i>	Disable logging and viewing of HTTP/S cache traffic.		
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-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
login-timestamp	Enable/disable login time recording.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable login time recording.		
	<i>disable</i>	Disable login time recording.		
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
special-file-23-support	Enable/disable detection of those special format files when using Data Loss Prevention.	option	-	disable

Parameter	Description	Type	Size	Default
	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.		
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable insertion of address UUID to traffic logs.		
	<i>disable</i>	Disable insertion of address UUID to traffic logs.		
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging of SSL connection events.		
	<i>disable</i>	Disable logging of SSL connection events.		
gui-rest-api-cache	Enable/disable REST API result caching on FortiProxy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable REST API result caching on FortiProxy.		
	<i>disable</i>	Disable REST API result caching on FortiProxy.		
rest-api-key-url-query	Enable/disable support for passing REST API keys through URL query parameters.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable support for passing REST API keys through URL query parameters.		
	<i>disable</i>	Disable support for passing REST API keys through URL query parameters.		
gui-cdn-domain-override	Domain of CDN server.	string	Maximum length: 255	

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
ha-affinity	Affinity setting for HA daemons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1
bfd-affinity	Affinity setting for BFD daemon (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1
cmdbsvr-affinity	Affinity setting for cmdbsvr (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1
av-affinity	Affinity setting for AV scanning (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
wad-affinity	Affinity setting for wad (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
ips-affinity	Affinity setting for IPS (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).	string	Maximum length: 79	0
miglog-affinity	Affinity setting for logging (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
syslog-affinity	Affinity setting for syslog (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0

Parameter	Description	Type	Size	Default						
url-filter-affinity	URL filter CPU affinity.	string	Maximum length: 79	0						
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						
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647	8192						
max-route-cache-size	Maximum number of IP route cache entries (0 - 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	0						
ipsec-round-robin	Enable/disable round-robin redistribution to multiple CPUs for IPsec VPN traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable round-robin redistribution for IPsec VPN.</td></tr><tr><td><i>disable</i></td><td>Disable round-robin redistribution for IPsec VPN.</td></tr></table>				Option	Description	<i>enable</i>	Enable round-robin redistribution for IPsec VPN.	<i>disable</i>	Disable round-robin redistribution for IPsec VPN.
Option	Description									
<i>enable</i>	Enable round-robin redistribution for IPsec VPN.									
<i>disable</i>	Disable round-robin redistribution for IPsec VPN.									
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						
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 20649 Maximum value: 58999	41299						
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 20649 Maximum value: 58999	41299						

Parameter	Description	Type	Size	Default						
user-device-store-max-unified-mem	Maximum unified memory allowed in user device store.	integer	Minimum value: 41299517 Maximum value: 412995174	206497587						
gui-device-latitude	Add the latitude of the location of this FortiProxy to position it on the Threat Map.	string	Maximum length: 19							
gui-device-longitude	Add the longitude of the location of this FortiProxy to position it on the Threat Map.	string	Maximum length: 19							
v-tpm	Enable/disable vTPM on VM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable vTPM.</td></tr><tr><td><i>enable</i></td><td>Enable vTPM</td></tr></table>				Option	Description	<i>disable</i>	Disable vTPM.	<i>enable</i>	Enable vTPM
Option	Description									
<i>disable</i>	Disable vTPM.									
<i>enable</i>	Enable vTPM									
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable private data encryption using an AES 128-bit key.</td></tr><tr><td><i>enable</i></td><td>Enable private data encryption using an AES 128-bit key.</td></tr></table>				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.
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.									
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><i>enable</i></td><td>Enable automatic authorization of dedicated Fortinet extension device globally.</td></tr><tr><td><i>disable</i></td><td>Disable automatic authorization of dedicated Fortinet extension device globally.</td></tr></table>				Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.
Option	Description									
<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.									
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.									
gui-theme	Color scheme for the administration GUI.	option	-	jade						

Parameter	Description	Type	Size	Default																								
	<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>retro</i></td><td>FortiProxy 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>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>retro</i>	FortiProxy v3 Retro 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>retro</i>	FortiProxy v3 Retro theme.																										
	<i>dark-matter</i>	Dark Matter theme.																										
	<i>onyx</i>	Onyx theme.																										
<i>eclipse</i>	Eclipse theme.																											
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yyyy/MM/dd</i></td><td>Year/Month/Day.</td></tr><tr><td><i>dd/MM/yyyy</i></td><td>Day/Month/Year.</td></tr><tr><td><i>MM/dd/yyyy</i></td><td>Month/Day/Year.</td></tr><tr><td><i>yyyy-MM-dd</i></td><td>Year-Month-Day.</td></tr><tr><td><i>dd-MM-yyyy</i></td><td>Day-Month-Year.</td></tr><tr><td><i>MM-dd-yyyy</i></td><td>Month-Day-Year.</td></tr></table>	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.													
	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.																											
gui-date-time-source	Source from which the FortiProxy GUI uses to display date and time entries.	option	-	system																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>system</i></td><td>Use this FortiProxy unit's configured timezone.</td></tr><tr><td><i>browser</i></td><td>Use the web browser's timezone.</td></tr></table>	Option	Description	<i>system</i>	Use this FortiProxy unit's configured timezone.	<i>browser</i>	Use the web browser's timezone.																					
	Option	Description																										
	<i>system</i>	Use this FortiProxy unit's configured timezone.																										
<i>browser</i>	Use the web browser's timezone.																											

Parameter	Description	Type	Size	Default
igmp-state-limit	Maximum number of IGMP memberships (96 - 64000, default = 3200).	integer	Minimum value: 96 Maximum value: 128000	3200
cloud-communication	Enable/disable all cloud communication.	option	-	enable
	Option	Description		
	<i>enable</i>	Allow cloud communication.		
	<i>disable</i>	Disable all cloud-related settings.		
ipsec-ha-seqjump-rate	ESP jump ahead rate (1G - 10G pps equivalent).	integer	Minimum value: 1 Maximum value: 10	10
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-	enable
	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
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
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Automatically switch CPU accounting mode.		
	<i>force</i>	Force the use of CPU IRQ time accounting mode.		
management-ip	Management IP address of this FortiProxy. Used to log into this FortiProxy from another FortiProxy in the Security Fabric.	string	Maximum length: 255	
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 1 Maximum value: 65535	443
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.		
forticonverter-integration	Enable/disable FortiConverter integration service.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiConverter integration service.		
	<i>disable</i>	Disable FortiConverter integration service.		
forticonverter-config-upload	Enable/disable config upload to FortiConverter.	option	-	disable
	Option	Description		
	<i>once</i>	Enable one-time config upload to FortiConverter.		
	<i>disable</i>	Disable config upload to FortiConverter.		

Parameter	Description	Type	Size	Default										
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><i>mini</i></td><td>Small sized Internet Service database with very limited IP addresses.</td></tr><tr><td><i>standard</i></td><td>Medium sized Internet Service database with most IP addresses.</td></tr><tr><td><i>full</i></td><td>Full sized Internet Service database with all IP addresses.</td></tr><tr><td><i>on-demand</i></td><td>Internet Service database with customer selected IP addresses.</td></tr></table>	Option	Description	<i>mini</i>	Small sized Internet Service database with very limited IP addresses.	<i>standard</i>	Medium sized Internet Service database with most IP addresses.	<i>full</i>	Full sized Internet Service database with all IP addresses.	<i>on-demand</i>	Internet Service database with customer selected IP addresses.			
Option	Description													
<i>mini</i>	Small sized Internet Service database with very limited IP addresses.													
<i>standard</i>	Medium sized Internet Service database with most IP addresses.													
<i>full</i>	Full sized Internet Service database with all IP addresses.													
<i>on-demand</i>	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											
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><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>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.	<i>disable</i>	Disable 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.													
<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.													
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><i>disable</i></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><i>enable</i></td><td>Allow use of the interface-subnet setting in firewall addresses.</td></tr></table>	Option	Description	<i>disable</i>	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.	<i>enable</i>	Allow use of the interface-subnet setting in firewall addresses.							
Option	Description													
<i>disable</i>	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.													
<i>enable</i>	Allow use of the interface-subnet setting in firewall addresses.													

Parameter	Description	Type	Size	Default						
sflowd-max-children-num	Maximum number of sflowd child processes allowed to run.	integer	Minimum value: 0 Maximum value: 6	6						
fortigslb-integration	Enable/disable integration with the FortiGSLB cloud service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable VIP and ZTNA server integration with the FortiGSLB cloud service.</td></tr><tr><td><i>enable</i></td><td>Enable VIP and ZTNA server integration with the FortiGSLB cloud service.</td></tr></table>	Option	Description	<i>disable</i>	Disable VIP and ZTNA server integration with the FortiGSLB cloud service.	<i>enable</i>	Enable VIP and ZTNA server integration with the FortiGSLB cloud service.			
	Option	Description								
	<i>disable</i>	Disable VIP and ZTNA server integration with the FortiGSLB cloud service.								
<i>enable</i>	Enable VIP and ZTNA server integration with the FortiGSLB cloud service.									
license-overlimit	System behaviour when max licensed proxy user is reached.	option	-	bypass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass further traffic when licensed user is reached.</td></tr><tr><td><i>block</i></td><td>Block further traffic when licensed user is reached.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass further traffic when licensed user is reached.	<i>block</i>	Block further traffic when licensed user is reached.			
	Option	Description								
	<i>bypass</i>	Bypass further traffic when licensed user is reached.								
<i>block</i>	Block further traffic when licensed user is reached.									
max-session-per-user	Max UTM sessions per user.	integer	Minimum value: 0 Maximum value: 4294967295	0						
conntrack	Max numbers of conntrack.	integer	Minimum value: 60000 Maximum value: 10000000	700000						
established-timeout	Default established session timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	1800						
time-wait-timeout	Default time-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60						

Parameter	Description	Type	Size	Default
fin-wait-timeout	Default fin-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
close-wait-timeout	Default close-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
syn-sent-timeout	Default syn-sent timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
syn-recv-timeout	Default syn-recv timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
last-ack-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	15
udp-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
udp-stream-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	180
username-case-sensitivity	Case sensitivity when performing username matching	option	-	enable
	OptionDescription			
	enable	Check case when performing username matching		
	disable	Ignore case when performing username matching		
tcp-random-source-port	Disable/Enable TCP IPv4 random source port.	option	-	disable
	OptionDescription			
	enable	Enable source port randomness.		
	disable	Disable source port randomness.		

config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set interface {string}
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address-any}
    set sequence-number-transmission [disable|enable]
    set sequence-number-reception [disable|enable]
    set checksum-transmission [disable|enable]
    set checksum-reception [disable|enable]
    set key-outbound {integer}
    set key-inbound {integer}
    set diffservcode {user}
    set keepalive-interval {integer}
    set keepalive-failtimes {integer}
  next
end
```

config system gre-tunnel

Parameter	Description	Type	Size	Default
name	Tunnel name.	string	Maximum length: 15	
interface	Interface name.	string	Maximum length: 15	
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified	0.0.0.0
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.	

Parameter	Description	Type	Size	Default
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.		
checksum-transmission	Enable/disable including checksums in transmitted GRE packets.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not include checksums in transmitted GRE packets.		
	<i>enable</i>	Include checksums in transmitted GRE packets.		
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.		
key-outbound	Include this key in transmitted GRE packets (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0
key-inbound	Require received GRE packets contain this key (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0
diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified	
keepalive-interval	Keepalive message interval (0 - 32767, 0 = disabled).	integer	Minimum value: 0 Maximum value: 32767	0
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

config system ha

Configure HA.

```
config system ha
  Description: Configure HA.
  set group-id {integer}
  set group-name {string}
  set mode [standalone|config-sync-only|...]
  set sync-packet-balance [enable|disable]
  set password {password}
  set key {password}
  set hbdev {user}
  set unicast-hb [enable|disable]
  set unicast-hb-peerip {ipv4-address}
  set unicast-hb-netmask {ipv4-netmask}
  set route-ttl {integer}
  set route-wait {integer}
  set route-hold {integer}
  set multicast-ttl {integer}
  set evpn-ttl {integer}
  set encryption [enable|disable]
  set authentication [enable|disable]
  set hb-interval {integer}
  set hb-interval-in-milliseconds [100ms|10ms]
  set hb-lost-threshold {integer}
  set hello-holddown {integer}
  set gratuitous-arps [enable|disable]
  set arps {integer}
  set arps-interval {integer}
  set link-failed-signal [enable|disable]
  set upgrade-mode [simultaneous|uninterruptible|...]
  set sequential-upgrade [enable|disable]
  set uninterruptible-primary-wait {integer}
  set primary-hold-before-reboot {integer}
  set ha-mgmt-status [enable|disable]
  config ha-mgmt-interfaces
    Description: Reserve interfaces to manage individual cluster units.
    edit <id>
      set interface {string}
      set dst {ipv4-classnet}
      set gateway {ipv4-address}
      set gateway6 {ipv6-address}
    next
  end
  set ha-uptime-diff-margin {integer}
  set unicast-status [enable|disable]
  set unicast-gateway {ipv4-address}
  config unicast-peers
    Description: Number of unicast peers.
    edit <id>
```

```

        set peer-ip {ipv4-address}
    next
end
set weight {user}
set cpu-threshold {user}
set memory-threshold {user}
set http-proxy-threshold {user}
set ftp-proxy-threshold {user}
set imap-proxy-threshold {user}
set nntp-proxy-threshold {user}
set pop3-proxy-threshold {user}
set smtp-proxy-threshold {user}
set override [enable|disable]
set priority {integer}
set override-wait-time {integer}
set monitor {user}
set pingserver-monitor-interface {user}
set pingserver-failover-threshold {integer}
set pingserver-secondary-force-reset [enable|disable]
set pingserver-flip-timeout {integer}
set vcluster-status [enable|disable]
config vcluster
    Description: Virtual cluster table.
    edit <vcluster-id>
        set override [enable|disable]
        set priority {integer}
        set override-wait-time {integer}
        set monitor {user}
        set pingserver-monitor-interface {user}
        set pingserver-failover-threshold {integer}
        set pingserver-secondary-force-reset [enable|disable]
        set pingserver-flip-timeout {integer}
        set vdom <name1>, <name2>, ...
    next
end
set ha-direct [enable|disable]
set ssd-failover [enable|disable]
set memory-compatible-mode [enable|disable]
set memory-based-failover [enable|disable]
set memory-failover-threshold {integer}
set memory-failover-monitor-period {integer}
set memory-failover-sample-rate {integer}
set memory-failover-flip-timeout {integer}
set failover-hold-time {integer}
set ipsec-phase2-proposal {option1}, {option2}, ...
end

```

config system ha

Parameter	Description	Type	Size	Default								
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									
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>Disable HA feature.</td></tr><tr><td><i>config-sync-only</i></td><td>Enable Config sync only</td></tr><tr><td><i>active-passive</i></td><td>Enable Active-passive mode.</td></tr></table>				Option	Description	<i>standalone</i>	Disable HA feature.	<i>config-sync-only</i>	Enable Config sync only	<i>active-passive</i>	Enable Active-passive mode.
Option	Description											
<i>standalone</i>	Disable HA feature.											
<i>config-sync-only</i>	Enable Config sync only											
<i>active-passive</i>	Enable Active-passive mode.											
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA packet distribution to multiple CPUs.</td></tr><tr><td><i>disable</i></td><td>Disable HA packet distribution to multiple CPUs.</td></tr></table>				Option	Description	<i>enable</i>	Enable HA packet distribution to multiple CPUs.	<i>disable</i>	Disable HA packet distribution to multiple CPUs.		
Option	Description											
<i>enable</i>	Enable HA packet distribution to multiple CPUs.											
<i>disable</i>	Disable HA packet distribution to multiple CPUs.											
password	Cluster password. Must be the same for all members.	password	Not Specified									
key	Key.	password	Not Specified									
hbdev	Heartbeat interfaces. Must be the same for all members.	user	Not Specified									
unicast-hb	Enable/disable unicast heartbeat.	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.											
unicast-hb-peerip	Unicast heartbeat peer IP.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default						
unicast-hb-netmask	Unicast heartbeat netmask.	ipv4-netmask	Not Specified	0.0.0.0						
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						
route-wait	Time to wait before sending new routes to the cluster (0 - 3600 sec).	integer	Minimum value: 0 Maximum value: 3600	0						
route-hold	Time to wait between routing table updates to the cluster (0 - 3600 sec).	integer	Minimum value: 0 Maximum value: 3600	10						
multicast-ttl	HA multicast TTL on primary (5 - 3600 sec).	integer	Minimum value: 5 Maximum value: 3600	600						
evpn-ttl	HA EVPN FDB TTL on primary box (5 - 3600 sec).	integer	Minimum value: 5 Maximum value: 3600	60						
encryption	Enable/disable heartbeat message encryption.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable heartbeat message encryption.</td></tr><tr><td><i>disable</i></td><td>Disable heartbeat message encryption.</td></tr></table>				Option	Description	<i>enable</i>	Enable heartbeat message encryption.	<i>disable</i>	Disable heartbeat message encryption.
Option	Description									
<i>enable</i>	Enable heartbeat message encryption.									
<i>disable</i>	Disable heartbeat message encryption.									
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.									
hb-interval	Time between sending heartbeat packets (1 - 20). Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2						

Parameter	Description	Type	Size	Default
hb-interval-in-milliseconds	Units of heartbeat interval time between sending heartbeat packets. Default is 100ms.	option	-	100ms
	Option	Description		
	100ms	Each heartbeat interval is 100ms.		
	10ms	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	20
hello-holddown	Time to wait before changing from hello to work state (5 - 300 sec).	integer	Minimum value: 5 Maximum value: 300	20
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-	enable
	Option	Description		
	enable	Enable gratuitous ARPs.		
	disable	Disable gratuitous ARPs.		
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
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
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

Parameter	Description	Type	Size	Default
upgrade-mode	The mode to upgrade a cluster.	option	-	uninterruptible
	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.		
sequential-upgrade	Enable to upgrade secondaries one by one.	option	-	enable
	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
primary-hold-before-reboot	Number of seconds the primary HA unit waits after the secondary HA unit upgraded and joined back HA then starts its own upgrade (0 - 600, default = 0).	integer	Minimum value: 0 Maximum value: 600	0
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-	disable
	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

Parameter	Description	Type	Size	Default						
unicast-status	Enable/disable unicast connection.	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.									
unicast-gateway	Default route gateway for unicast interface.	ipv4-address	Not Specified	0.0.0.0						
weight	Weight-round-robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified	0 40						
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified							
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified							
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified							
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP 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							
nnntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified							
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified							

Parameter	Description	Type	Size	Default						
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP 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.									
priority	Increase the priority to select the primary unit (0 - 255).	integer	Minimum value: 0 Maximum value: 255	128						
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						
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified							
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified							
pingserver-failover-threshold	Remote IP monitoring failover threshold (0 - 50).	integer	Minimum value: 0 Maximum value: 50	0						
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable force reset of secondary member after PING server failure.</td></tr><tr><td><i>disable</i></td><td>Disable force reset of secondary member after PING server failure.</td></tr></table>				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.
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.									

Parameter	Description	Type	Size	Default						
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60						
vcluster-status	Enable/disable virtual cluster for virtual clustering.	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-direct	Enable/disable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.</td></tr><tr><td><i>disable</i></td><td>Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.</td></tr></table>	Option	Description	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.	<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.			
Option	Description									
<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.									
<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.									
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.									
memory-compatible-mode	Enable/disable memory compatible 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.									
memory-based-failover	Enable/disable memory based failover.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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-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-flip-timeout	Time to wait between subsequent memory based failovers in minutes (6 - 2147483647, default = 6).	integer	Minimum value: 6 Maximum value: 2147483647	6
failover-hold-time	Time to wait before failover (0 - 300 sec, default = 0), to avoid flip.	integer	Minimum value: 0 Maximum value: 300	0
ipsec-phase2-proposal	IPsec phase2 proposal.	option	-	
	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		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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		

config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface to reserve for HA management.	string	Maximum length: 15	
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
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	::

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
vcluster-id	ID.	integer	Minimum value: 1 Maximum value: 30	1
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.		
priority	Increase the priority to select the primary unit (0 - 255).	integer	Minimum value: 0 Maximum value: 255	128
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
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold (0 - 50).	integer	Minimum value: 0 Maximum value: 50	0
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable
	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.		

Parameter	Description	Type	Size	Default
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60
vdom <name>	Virtual domain(s) in the virtual cluster. Virtual domain name.	string	Maximum length: 79	

config system ha-lic

ha-lic

```
config system ha-lic
  Description: ha-lic
  edit <serial-num>
    set last-sync-time {password}
    set last-sync-seat {password}
    set last-sync-seat-fnbi {password}
    set last-sync-seat-fcas {password}
  next
end
```

config system ha-lic

Parameter	Description	Type	Size	Default
serial-num	The Serial Number that joined an HA cluster.	string	Maximum length: 16	
last-sync-time	Last time_t when SN updated the user seats.	password	Not Specified	
last-sync-seat	Last seats when SN updated the user seats.	password	Not Specified	
last-sync-seat-fnbi	Last seats when SN updated the isolator seats.	password	Not Specified	
last-sync-seat-fcas	Last seats when SN updated the image AI seats.	password	Not Specified	

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
	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
vlan-hb-lost-threshold	VLAN lost heartbeat threshold (1 - 60).	integer	Minimum value: 1 Maximum value: 60	3

config system ha-nonsync-csum

System checksum for FortiManager use only.

```

config system ha-nonsync-csum
    Description: System checksum for FortiManager use only.
end

```

config system info admin ssh

Show SSH status.

```

config system info admin ssh
    Description: Show SSH status.
end

```

config system info admin status

Show logged in administrators.

```
config system info admin status
    Description: Show logged in administrators.
end
```

config system interface

Configure interfaces.

```
config system interface
    Description: Configure interfaces.
    edit <name>
        set vdom {string}
        set cli-conn-status {integer}
        set mode [static|dhcp|...]
        config client-options
            Description: DHCP client options.
            edit <id>
                set code {integer}
                set type [hex|string|...]
                set value {string}
                set ip {user}
            next
        end
        set distance {integer}
        set priority {integer}
        set dhcp-relay-interface-select-method [auto|specify]
        set dhcp-relay-interface {string}
        set dhcp-broadcast-flag [disable|enable]
        set dhcp-relay-service [disable|enable]
        set dhcp-relay-ip {user}
        set dhcp-relay-source-ip {ipv4-address}
        set dhcp-relay-circuit-id {string}
        set dhcp-relay-link-selection {ipv4-address}
        set dhcp-relay-request-all-server [disable|enable]
        set dhcp-relay-allow-no-end-option [disable|enable]
        set dhcp-relay-type [regular|ipsec]
        set dhcp-smart-relay [disable|enable]
        set dhcp-relay-agent-option [enable|disable]
        set dhcp-classless-route-addition [enable|disable]
        set management-ip {ipv4-classnet-host}
        set ip {ipv4-classnet-host}
        set allowaccess {option1}, {option2}, ...
        set gwdetect [enable|disable]
        set ping-serv-status {integer}
        set detectserver {user}
```



```

set detectprotocol {option1}, {option2}, ...
set ha-priority {integer}
set fail-detect [enable|disable]
set fail-detect-option {option1}, {option2}, ...
set fail-alert-method [link-failed-signal|link-down]
set fail-action-on-extender [soft-restart|hard-restart|...]
set fail-alert-interfaces <name1>, <name2>, ...
set dhcp-client-identifier {string}
set dhcp-renew-time {integer}
set ipunnumbered {ipv4-address}
set username {string}
set pppoe-egress-cos [cos0|cos1|...]
set pppoe-unnumbered-negotiate [enable|disable]
set password {password}
set idle-timeout {integer}
set detected-peer-mtu {integer}
set disc-retry-timeout {integer}
set padt-retry-timeout {integer}
set service-name {string}
set ac-name {string}
set lcp-echo-interval {integer}
set lcp-max-echo-fails {integer}
set defaultgw [enable|disable]
set dns-server-override [enable|disable]
set dns-server-protocol {option1}, {option2}, ...
set auth-type [auto|pap|...]
set pptp-client [enable|disable]
set pptp-user {string}
set pptp-password {password}
set pptp-server-ip {ipv4-address}
set pptp-auth-type [auto|pap|...]
set pptp-timeout {integer}
set arpforward [enable|disable]
set broadcast-forward [enable|disable]
set bfd [global|enable|...]
set bfd-desired-min-tx {integer}
set bfd-detect-mult {integer}
set bfd-required-min-rx {integer}
set l2forward [enable|disable]
set icmp-send-redirect [enable|disable]
set icmp-accept-redirect [enable|disable]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set macaddr {mac-address}
set substitute-dst-mac {mac-address}
set large-receive-offload [enable|disable]
set generic-receive-offload [enable|disable]
set speed [auto|10full|...]
set status [up|down]
set netbios-forward [disable|enable]
set wins-ip {ipv4-address}
set type [physical|vlan|...]

```

```

set dedicated-to [none|management]
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 ring-rx {integer}
set ring-tx {integer}
set wccp [enable|disable]
set drop-overlapped-fragment [enable|disable]
set drop-fragment [enable|disable]
set src-check [enable|disable]
set explicit-web-proxy [enable|disable]
set explicit-ftp-proxy [enable|disable]
set proxy-captive-portal [enable|disable]
set tcp-mss {integer}
set inbandwidth {integer}
set outbandwidth {integer}
set egress-shaping-profile {string}
set ingress-shaping-profile {string}
set spillover-threshold {integer}
set ingress-spillover-threshold {integer}
set weight {integer}
set interface {string}
set external [enable|disable]
set mtu-override [enable|disable]
set mtu {integer}
set vlan-protocol [8021q|8021ad]
set vlanid {integer}
set forward-domain {integer}
set remote-ip {ipv4-classnet-host}
set member <interface-name1>, <interface-name2>, ...
set lacp-mode {option}
set lacp-ha-secondary [enable|disable]
set system-id-type [auto|user]
set system-id {mac-address}
set lacp-speed [slow|fast]
set min-links {integer}
set min-links-down [operational|administrative]
set algorithm [L2|L3|...]
set link-up-delay {integer}
set aggregate-type [physical|vxlan]
set priority-override [enable|disable]
set aggregate {string}
set redundant-interface {string}
set devindex {integer}
set switch {string}
set description {var-string}
set alias {string}
set security-mode [none|captive-portal|...]
set security-mac-auth-bypass [mac-auth-only|enable|...]

```

```

set security-external-web {var-string}
set security-external-logout {string}
set replacemsg-override-group {string}
set security-redirect-url {var-string}
set auth-cert {string}
set auth-portal-addr {string}
set security-exempt-list {string}
set security-groups <name1>, <name2>, ...
set ike-saml-server {string}
config phy-setting
    Description: PHY settings
    set signal-ok-threshold-value {integer}
end
set role [lan|wan|...]
set snmp-index {integer}
set secondary-IP [enable|disable]
config secondaryip
    Description: Second IP address of interface.
    edit <id>
        set ip {ipv4-classnet-host}
        set secip-relay-ip {user}
        set allowaccess {option1}, {option2}, ...
        set gwdetect [enable|disable]
        set ping-serv-status {integer}
        set detectserver {user}
        set detectprotocol {option1}, {option2}, ...
        set ha-priority {integer}
    next
end
set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set eap-supPLICant [enable|disable]
set eap-method [tls|peap]
set eap-identity {string}
set eap-password {password}
set eap-ca-cert {string}
set eap-user-cert {string}
set default-purdue-level [1|1.5|...]
config ipv6
    Description: IPv6 of interface.
    set ip6-mode [static|dhcp|...]
    set nd-mode [basic|SEND-compatible]
    set nd-cert {string}
    set nd-security-level {integer}
    set nd-timestamp-delta {integer}
    set nd-timestamp-fuzz {integer}

```

```

set nd-cga-modifier {user}
set ip6-dns-server-override [enable|disable]
set ip6-address {ipv6-prefix}
config ip6-extra-addr
    Description: Extra IPv6 address prefixes of interface.
    edit <prefix>
        next
    end
set ip6-allowaccess {option1}, {option2}, ...
set ip6-send-adv [enable|disable]
set icmp6-send-redirect [enable|disable]
set ip6-manage-flag [enable|disable]
set ip6-other-flag [enable|disable]
set ip6-max-interval {integer}
set ip6-min-interval {integer}
set ip6-link-mtu {integer}
set ra-send-mtu [enable|disable]
set ip6-reachable-time {integer}
set ip6-retrans-time {integer}
set ip6-default-life {integer}
set ip6-hop-limit {integer}
set autoconf [enable|disable]
set unique-autoconf-addr [enable|disable]
set interface-identifier {ipv6-address}
set ip6-prefix-mode [dhcp6|ra]
set ip6-delegated-prefix-iaid {integer}
set ip6-upstream-interface {string}
set ip6-subnet {ipv6-prefix}
config ip6-prefix-list
    Description: Advertised prefix list.
    edit <prefix>
        set autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set valid-life-time {integer}
        set preferred-life-time {integer}
        set rdns {user}
        set dnssl <domain1>, <domain2>, ...
    next
end
config ip6-delegated-prefix-list
    Description: Advertised IPv6 delegated prefix list.
    edit <prefix-id>
        set upstream-interface {string}
        set delegated-prefix-iaid {integer}
        set autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set subnet {ipv6-network}
        set rdns-service [delegated|default|...]
        set rdns {user}
    next
end
set dhcp6-relay-service [disable|enable]

```

```

set dhcp6-relay-type {option}
set dhcp6-relay-source-interface [disable|enable]
set dhcp6-relay-ip {user}
set dhcp6-relay-source-ip {ipv6-address}
set dhcp6-relay-interface-id {string}
set dhcp6-client-options {option1}, {option2}, ...
set dhcp6-prefix-delegation [enable|disable]
set dhcp6-information-request [enable|disable]
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 cli-conn6-status {integer}
end
next
end

```

config system interface

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 15									
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31									
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0								
mode	Addressing mode (static, DHCP, PPPoE).	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>External DHCP client mode.</td></tr><tr><td><i>pppoe</i></td><td>External PPPoE mode.</td></tr></table>				Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	External DHCP client mode.	<i>pppoe</i>	External PPPoE mode.
Option	Description											
<i>static</i>	Static setting.											
<i>dhcp</i>	External DHCP client mode.											
<i>pppoe</i>	External PPPoE mode.											

Parameter	Description	Type	Size	Default
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255	5
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	0
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>specify</i>		Set outgoing interface manually.	
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-broadcast-flag	Enable/disable setting of the broadcast flag in messages sent by the DHCP client (default = enable).	option	-	enable
	Option		Description	
	<i>disable</i>		Disable broadcast flag.	
	<i>enable</i>		Enable broadcast flag.	
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-ip	DHCP relay IP address.	user	Not Specified	
dhcp-relay-source-ip	IP address used by the DHCP relay as its source IP.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
dhcp-relay-circuit-id	DHCP relay circuit ID.	string	Maximum length: 64							
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Send DHCP requests only to a matching server.</td></tr><tr><td>enable</td><td>Send DHCP requests to all servers.</td></tr></table>	Option	Description	disable	Send DHCP requests only to a matching server.	enable	Send DHCP requests to all servers.			
Option	Description									
disable	Send DHCP requests only to a matching server.									
enable	Send DHCP requests to all servers.									
dhcp-relay-allow-no-end-option	Enable/disable relaying DHCP messages with no end option.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable relaying DHCP messages with no end option.</td></tr><tr><td>enable</td><td>Enable relaying DHCP messages with no end option.</td></tr></table>	Option	Description	disable	Disable relaying DHCP messages with no end option.	enable	Enable relaying DHCP messages with no end option.			
Option	Description									
disable	Disable relaying DHCP messages with no end option.									
enable	Enable relaying DHCP messages with no end option.									
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>regular</td><td>Regular DHCP relay.</td></tr><tr><td>ipsec</td><td>DHCP relay for IPsec.</td></tr></table>	Option	Description	regular	Regular DHCP relay.	ipsec	DHCP relay for IPsec.			
Option	Description									
regular	Regular DHCP relay.									
ipsec	DHCP relay for IPsec.									
dhcp-smart-relay	Enable/disable DHCP smart relay.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DHCP smart relay.</td></tr><tr><td>enable</td><td>Enable DHCP smart relay.</td></tr></table>	Option	Description	disable	Disable DHCP smart relay.	enable	Enable DHCP smart relay.			
Option	Description									
disable	Disable DHCP smart relay.									
enable	Enable DHCP smart relay.									
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DHCP relay agent option.</td></tr><tr><td>disable</td><td>Disable DHCP relay agent option.</td></tr></table>	Option	Description	enable	Enable DHCP relay agent option.	disable	Disable DHCP relay agent option.			
Option	Description									
enable	Enable DHCP relay agent option.									
disable	Disable DHCP relay agent option.									

Parameter	Description	Type	Size	Default																										
dhcp-classless-route-addition	Enable/disable addition of classless static routes retrieved from DHCP server.	option	-	enable																										
	<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.																													
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																										
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																										
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><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></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.	<i>speed-test</i>	Speed test 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.																													
<i>speed-test</i>	Speed test access.																													
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable																										

Parameter	Description	Type	Size	Default								
	<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.											
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0								
detectserver	Gateway's ping server for this IP.	user	Not Specified									
detectprotocol	Protocols used to detect the server.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo.</td></tr></table>	Option	Description	<i>ping</i>	PING.	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.			
Option	Description											
<i>ping</i>	PING.											
<i>tcp-echo</i>	TCP echo.											
<i>udp-echo</i>	UDP echo.											
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1								
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								
	<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.											
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-	link-down								

Parameter	Description	Type	Size	Default								
	<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-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 FortiProxy interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 15									
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48									
dhcp-renew-time	DHCP renew time in seconds (300-604800), 0 means use the renew time provided by the server.	integer	Minimum value: 300 Maximum value: 604800	0								
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified	0.0.0.0								
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64									
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><i>cos0</i></td><td>CoS 0.</td></tr><tr><td><i>cos1</i></td><td>CoS 1.</td></tr></table>	Option	Description	<i>cos0</i>	CoS 0.	<i>cos1</i>	CoS 1.					
	Option	Description										
	<i>cos0</i>	CoS 0.										
<i>cos1</i>	CoS 1.											

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></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>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>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.																	
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP address negotiating for unnumbered.</td></tr><tr><td><i>disable</i></td><td>Disable IP address negotiating for unnumbered.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP address negotiating for unnumbered.	<i>disable</i>	Disable IP address negotiating for unnumbered.											
	Option	Description																
	<i>enable</i>	Enable IP address negotiating for unnumbered.																
<i>disable</i>	Disable IP address negotiating for unnumbered.																	
password	PPPoE account's password.	password	Not Specified															
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 32767	0														
detected-peer-mtu	MTU of detected peer (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0														
disc-retry-timeout	Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 4294967295	1														
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295	1														
service-name	PPPoE service name.	string	Maximum length: 63															

Parameter	Description	Type	Size	Default								
ac-name	PPPoE server name.	string	Maximum length: 63									
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								
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><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.											
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Use DNS acquired by DHCP or PPPoE.</td></tr><tr><td><i>disable</i></td><td>No not use DNS acquired by DHCP or PPPoE.</td></tr></table>	Option	Description	<i>enable</i>	Use DNS acquired by DHCP or PPPoE.	<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.					
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								
	<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.											
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></table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.					
Option	Description											
<i>auto</i>	Automatically choose authentication.											
<i>pap</i>	PAP authentication.											

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></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	chap	CHAP authentication.	mschapv1	MS-CHAPv1 authentication.	mschapv2	MS-CHAPv2 authentication.							
	Option	Description														
	chap	CHAP authentication.														
	mschapv1	MS-CHAPv1 authentication.														
mschapv2	MS-CHAPv2 authentication.															
pptp-client	Enable/disable PPTP client.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable PPTP client.</td></tr><tr><td>disable</td><td>Disable PPTP client.</td></tr></table>	Option	Description	enable	Enable PPTP client.	disable	Disable PPTP client.									
	Option	Description														
	enable	Enable PPTP client.														
disable	Disable PPTP client.															
pptp-user	PPTP user name.	string	Maximum length: 64													
pptp-password	PPTP password.	password	Not Specified													
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0												
pptp-auth-type	PPTP authentication type.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatically choose authentication.</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 authentication.	pap	PAP authentication.	chap	CHAP authentication.	mschapv1	MS-CHAPv1 authentication.	mschapv2	MS-CHAPv2 authentication.			
	Option	Description														
	auto	Automatically choose authentication.														
	pap	PAP authentication.														
	chap	CHAP authentication.														
	mschapv1	MS-CHAPv1 authentication.														
mschapv2	MS-CHAPv2 authentication.															
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0												
arpforward	Enable/disable ARP forwarding.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ARP forwarding.</td></tr><tr><td>disable</td><td>Disable ARP forwarding.</td></tr></table>	Option	Description	enable	Enable ARP forwarding.	disable	Disable ARP forwarding.									
	Option	Description														
	enable	Enable ARP forwarding.														
disable	Disable ARP forwarding.															
broadcast-forward	Enable/disable broadcast forwarding.	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 forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast forwarding.	<i>disable</i>	Disable broadcast forwarding.					
	Option	Description										
	<i>enable</i>	Enable broadcast forwarding.										
<i>disable</i>	Disable broadcast forwarding.											
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.											
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								
l2forward	Enable/disable l2 forwarding.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable L2 forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable L2 forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable L2 forwarding.	<i>disable</i>	Disable L2 forwarding.					
	Option	Description										
	<i>enable</i>	Enable L2 forwarding.										
<i>disable</i>	Disable L2 forwarding.											
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.											

Parameter	Description	Type	Size	Default								
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.											
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><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-all-ext-id</i>	Replace all extension IDs (root, bridge).	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.	<i>rpl-nothing</i>	Replace nothing.			
Option	Description											
<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).											
<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.											
<i>rpl-nothing</i>	Replace nothing.											
macaddr	Change the interface's MAC address.	mac-address	Not Specified	00:00:00:00:00:00								
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								
large-receive-offload	Enable/disable large-receive-offload.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable large-receive-offload.</td></tr><tr><td><i>disable</i></td><td>Disable large-receive-offload.</td></tr></table>	Option	Description	<i>enable</i>	Enable large-receive-offload.	<i>disable</i>	Disable large-receive-offload.					
Option	Description											
<i>enable</i>	Enable large-receive-offload.											
<i>disable</i>	Disable large-receive-offload.											
generic-receive-offload	Enable/disable generic-receive-offload.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable generic-receive-offload.</td></tr><tr><td><i>disable</i></td><td>Disable generic-receive-offload.</td></tr></table>	Option	Description	<i>enable</i>	Enable generic-receive-offload.	<i>disable</i>	Disable generic-receive-offload.					
Option	Description											
<i>enable</i>	Enable generic-receive-offload.											
<i>disable</i>	Disable generic-receive-offload.											

Parameter	Description	Type	Size	Default																														
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><i>auto</i></td><td>Automatically adjust speed.</td></tr><tr><td><i>10full</i></td><td>10M full-duplex.</td></tr><tr><td><i>10half</i></td><td>10M half-duplex.</td></tr><tr><td><i>100full</i></td><td>100M full-duplex.</td></tr><tr><td><i>100half</i></td><td>100M half-duplex.</td></tr><tr><td><i>100auto</i></td><td>100M auto-negotiation.</td></tr><tr><td><i>1000full</i></td><td>1000M full-duplex.</td></tr><tr><td><i>1000auto</i></td><td>1000M auto adjust.</td></tr><tr><td><i>2500auto</i></td><td>2500M auto-negotiation.</td></tr><tr><td><i>5000auto</i></td><td>5000M auto-negotiation.</td></tr><tr><td><i>50000full</i></td><td>50G full-duplex.</td></tr><tr><td><i>50000auto</i></td><td>50G auto-negotiation.</td></tr><tr><td><i>200Gfull</i></td><td>200G full-duplex.</td></tr><tr><td><i>200Gauto</i></td><td>200G auto-negotiation.</td></tr></table>	Option	Description	<i>auto</i>	Automatically adjust speed.	<i>10full</i>	10M full-duplex.	<i>10half</i>	10M half-duplex.	<i>100full</i>	100M full-duplex.	<i>100half</i>	100M half-duplex.	<i>100auto</i>	100M auto-negotiation.	<i>1000full</i>	1000M full-duplex.	<i>1000auto</i>	1000M auto adjust.	<i>2500auto</i>	2500M auto-negotiation.	<i>5000auto</i>	5000M auto-negotiation.	<i>50000full</i>	50G full-duplex.	<i>50000auto</i>	50G auto-negotiation.	<i>200Gfull</i>	200G full-duplex.	<i>200Gauto</i>	200G auto-negotiation.			
Option	Description																																	
<i>auto</i>	Automatically adjust speed.																																	
<i>10full</i>	10M full-duplex.																																	
<i>10half</i>	10M half-duplex.																																	
<i>100full</i>	100M full-duplex.																																	
<i>100half</i>	100M half-duplex.																																	
<i>100auto</i>	100M auto-negotiation.																																	
<i>1000full</i>	1000M full-duplex.																																	
<i>1000auto</i>	1000M auto adjust.																																	
<i>2500auto</i>	2500M auto-negotiation.																																	
<i>5000auto</i>	5000M auto-negotiation.																																	
<i>50000full</i>	50G full-duplex.																																	
<i>50000auto</i>	50G auto-negotiation.																																	
<i>200Gfull</i>	200G full-duplex.																																	
<i>200Gauto</i>	200G auto-negotiation.																																	
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.																																	
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable																														
	<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.																																	
wins-ip	WINS server IP.	ipv4-address	Not Specified	0.0.0.0																														

Parameter	Description	Type	Size	Default																		
type	Interface type.	option	-	vlan																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>physical</i></td><td>Physical interface.</td></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>loopback</i></td><td>Loopback interface.</td></tr><tr><td><i>vdom-link</i></td><td>VDOM link interface.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN interface.</td></tr></table>	Option	Description	<i>physical</i>	Physical interface.	<i>vlan</i>	VLAN interface.	<i>aggregate</i>	Aggregate interface.	<i>redundant</i>	Redundant interface.	<i>tunnel</i>	Tunnel interface.	<i>loopback</i>	Loopback interface.	<i>vdom-link</i>	VDOM link interface.	<i>vxlan</i>	VXLAN interface.			
	Option	Description																				
	<i>physical</i>	Physical interface.																				
	<i>vlan</i>	VLAN interface.																				
	<i>aggregate</i>	Aggregate interface.																				
	<i>redundant</i>	Redundant interface.																				
	<i>tunnel</i>	Tunnel interface.																				
	<i>loopback</i>	Loopback interface.																				
	<i>vdom-link</i>	VDOM link interface.																				
<i>vxlan</i>	VXLAN interface.																					
dedicated-to	Configure interface for single purpose.	option	-	none																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Interface not dedicated for any purpose.</td></tr><tr><td><i>management</i></td><td>Dedicate this interface for management purposes only.</td></tr></table>	Option	Description	<i>none</i>	Interface not dedicated for any purpose.	<i>management</i>	Dedicate this interface for management purposes only.															
	Option	Description																				
	<i>none</i>	Interface not dedicated for any purpose.																				
<i>management</i>	Dedicate this interface for management purposes only.																					
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																		

Parameter	Description	Type	Size	Default						
ring-rx	RX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ring-tx	TX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable drop of overlapped fragment packets.</td></tr><tr><td><i>disable</i></td><td>Disable drop of overlapped fragment packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable drop of overlapped fragment packets.	<i>disable</i>	Disable drop of overlapped fragment packets.			
Option	Description									
<i>enable</i>	Enable drop of overlapped fragment packets.									
<i>disable</i>	Disable drop of overlapped fragment packets.									
drop-fragment	Enable/disable drop fragment packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable/disable drop fragment packets.</td></tr><tr><td><i>disable</i></td><td>Do not drop fragment packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable/disable drop fragment packets.	<i>disable</i>	Do not drop fragment packets.			
Option	Description									
<i>enable</i>	Enable/disable drop fragment packets.									
<i>disable</i>	Do not drop fragment packets.									
src-check	Enable/disable source IP check.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source IP check.</td></tr><tr><td><i>disable</i></td><td>Disable source IP check.</td></tr></table>	Option	Description	<i>enable</i>	Enable source IP check.	<i>disable</i>	Disable source IP check.			
Option	Description									
<i>enable</i>	Enable source IP check.									
<i>disable</i>	Disable source IP check.									

Parameter	Description	Type	Size	Default						
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit Web proxy on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable explicit Web proxy on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit Web proxy on this interface.	<i>disable</i>	Disable explicit Web proxy on this interface.			
Option	Description									
<i>enable</i>	Enable explicit Web proxy on this interface.									
<i>disable</i>	Disable explicit Web proxy on this interface.									
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit FTP proxy on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable explicit FTP proxy on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit FTP proxy on this interface.	<i>disable</i>	Disable explicit FTP proxy on this interface.			
Option	Description									
<i>enable</i>	Enable explicit FTP proxy on this interface.									
<i>disable</i>	Disable explicit FTP proxy on this interface.									
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable proxy captive portal on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable proxy captive portal on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable proxy captive portal on this interface.	<i>disable</i>	Disable proxy captive portal on this interface.			
Option	Description									
<i>enable</i>	Enable proxy captive portal on this interface.									
<i>disable</i>	Disable proxy captive portal on this interface.									
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 48 Maximum value: 65535	0						
inbandwidth	Bandwidth limit for incoming traffic (0 - 80000000 kbps), 0 means unlimited.	integer	Minimum value: 0 Maximum value: 80000000	0						
outbandwidth	Bandwidth limit for outgoing traffic (0 - 80000000 kbps).	integer	Minimum value: 0 Maximum value: 80000000	0						
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35							
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
spillover-threshold	Egress Spillover threshold (0 - 16776000 kbps), 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						
ingress-spillover-threshold	Ingress Spillover threshold (0 - 16776000 kbps), 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255	0						
interface	Interface name.	string	Maximum length: 15							
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.									
mtu-override	Enable to set a custom MTU for this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override default MTU.</td></tr><tr><td><i>disable</i></td><td>Use default MTU.</td></tr></table>				Option	Description	<i>enable</i>	Override default MTU.	<i>disable</i>	Use default MTU.
Option	Description									
<i>enable</i>	Override default MTU.									
<i>disable</i>	Use default MTU.									
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500						
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>8021q</i>	IEEE 802.1Q.		
	<i>8021ad</i>	IEEE 802.1AD.		
vlanid	VLAN ID (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094	0
forward-domain	Transparent mode forward domain.	integer	Minimum value: 1 Maximum value: 4094	1
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
member <interface-name>	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79	
lACP-mode	LACP mode.	option	-	
	Option	Description		
	<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.		
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.		
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.		

Parameter	Description	Type	Size	Default										
system-id	Define a system ID for the aggregate interface.	mac-address	Not Specified	00:00:00:00:00:00										
lacp-speed	How often the interface sends LACP messages.	option	-	slow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>slow</i></td><td>Send LACP message every 30 seconds.</td></tr><tr><td><i>fast</i></td><td>Send LACP message every second.</td></tr></table>	Option	Description	<i>slow</i>	Send LACP message every 30 seconds.	<i>fast</i>	Send LACP message every second.							
Option	Description													
<i>slow</i>	Send LACP message every 30 seconds.													
<i>fast</i>	Send LACP message every second.													
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32	1										
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.													
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.													
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50										
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></table>	Option	Description	<i>physical</i>	Physical interface aggregation.									
Option	Description													
<i>physical</i>	Physical interface aggregation.													

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vxlan</i></td><td>VXLAN interface aggregation.</td></tr></table>	Option	Description	<i>vxlan</i>	VXLAN interface aggregation.							
Option	Description											
<i>vxlan</i>	VXLAN interface aggregation.											
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fail back to higher priority port once recovered.</td></tr><tr><td><i>disable</i></td><td>Disable fail back to higher priority port once recovered.</td></tr></table>	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.					
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.											
aggregate	Aggregate interface.	string	Maximum length: 15									
redundant-interface	Redundant interface.	string	Maximum length: 15									
devindex	Device Index.	integer	Minimum value: 0 Maximum value: 4294967295	0								
switch	Contained in switch.	string	Maximum length: 15									
description	Description.	var-string	Maximum length: 255									
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25									
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-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable								

Parameter	Description	Type	Size	Default
	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.		
security-external-web	URL of external authentication web server.	var-string	Maximum length: 1023	
security-external-logout	URL of external authentication logout server.	string	Maximum length: 127	
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35	
security-redirect-url	URL redirection after disclaimer/authentication.	var-string	Maximum length: 1023	
auth-cert	HTTPS server certificate.	string	Maximum length: 35	
auth-portal-addr	Address of captive portal.	string	Maximum length: 63	
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35	
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	
ike-saml-server	Configure IKE authentication SAML server.	string	Maximum length: 35	
role	Interface role.	option	-	undefined
	Option	Description		
	<i>lan</i>	Connected to local network of endpoints.		
	<i>wan</i>	Connected to Internet.		
	<i>dmz</i>	Connected to server zone.		
	<i>undefined</i>	Interface has no specific role.		

Parameter	Description	Type	Size	Default						
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 1 Maximum value: 2147483647	0						
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secondary IP.</td></tr><tr><td><i>disable</i></td><td>Disable secondary IP.</td></tr></table>	Option	Description	<i>enable</i>	Enable secondary IP.	<i>disable</i>	Disable secondary IP.			
Option	Description									
<i>enable</i>	Enable secondary IP.									
<i>disable</i>	Disable secondary IP.									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
eap-supplicant	Enable/disable EAP-Supplicant.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAP Supplicant.</td></tr><tr><td><i>disable</i></td><td>Disable EAP Supplicant.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAP Supplicant.	<i>disable</i>	Disable EAP Supplicant.			
Option	Description									
<i>enable</i>	Enable EAP Supplicant.									
<i>disable</i>	Disable EAP Supplicant.									
eap-method	EAP method.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls</i></td><td>TLS.</td></tr><tr><td><i>peap</i></td><td>PEAP.</td></tr></table>	Option	Description	<i>tls</i>	TLS.	<i>peap</i>	PEAP.			
Option	Description									
<i>tls</i>	TLS.									
<i>peap</i>	PEAP.									
eap-identity	EAP identity.	string	Maximum length: 35							
eap-password	EAP password.	password	Not Specified							
eap-ca-cert	EAP CA certificate name.	string	Maximum length: 79							
eap-user-cert	EAP user certificate name.	string	Maximum length: 35							
default-purdue-level	default purdue level of device detected on this interface.	option	-	3						

Parameter	Description	Type	Size	Default
	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		

config client-options

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
code	DHCP client option code.	integer	Minimum value: 0 Maximum value: 255	0
type	DHCP client 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.		
value	DHCP client option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

config phy-setting

Parameter	Description	Type	Size	Default
signal-ok-threshold-value	Signal-ok-threshold value(0 - 12).	integer	Minimum value: 0 Maximum value: 12	0

config secondaryip

Parameter	Description	Type	Size	Default
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
secip-relay-ip	DHCP relay IP address.	user	Not Specified	
allowaccess	Management access settings for the secondary IP address.	option	-	
		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.	
		<i>speed-test</i>	Speed test access.	

Parameter	Description	Type	Size	Default
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable detect gateway alive for first.		
	<i>disable</i>	Disable detect gateway alive for first.		
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0
detectserver	Gateway's ping server for this IP.	user	Not Specified	
detectprotocol	Protocols used to detect the server.	option	-	ping
	Option	Description		
	<i>ping</i>	PING.		
	<i>tcp-echo</i>	TCP echo.		
	<i>udp-echo</i>	UDP echo.		
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1

config tagging

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

config ipv6

Parameter	Description	Type	Size	Default
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-	static

Parameter	Description	Type	Size	Default										
	<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.													
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.													
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35											
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										
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified											
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><i>enable</i></td><td>Enable using the DNS server acquired by DHCP.</td></tr><tr><td><i>disable</i></td><td>Disable using the DNS server acquired by DHCP.</td></tr></table>	Option	Description	<i>enable</i>	Enable using the DNS server acquired by DHCP.	<i>disable</i>	Disable using the DNS server acquired by DHCP.							
	Option	Description												
	<i>enable</i>	Enable using the DNS server acquired by DHCP.												
<i>disable</i>	Disable using the DNS server acquired by DHCP.													
ip6-address	Primary IPv6 address prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx x.	ipv6-prefix	Not Specified	::/0										

Parameter	Description	Type	Size	Default																		
ip6-allowaccess	Allow management access to the 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>fabric</i></td><td>Fabric 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>fabric</i>	Fabric 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>fabric</i>	Fabric access.																					
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.																					
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.																					
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-other-flag	Enable/disable the other IPv6 flag.	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 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-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-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000	0						
ra-send-mtu	Enable/disable sending link MTU in RA packet.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending link MTU in RA packet.</td></tr><tr><td><i>disable</i></td><td>Disable sending link MTU in RA packet.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending link MTU in RA packet.	<i>disable</i>	Disable sending link MTU in RA packet.			
	Option	Description								
	<i>enable</i>	Enable sending link MTU in RA packet.								
<i>disable</i>	Disable sending link MTU in RA packet.									
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-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000	1800						
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255	0						

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.									
unique-autoconf-addr	Enable/disable unique auto config address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unique auto-configuration address.</td></tr><tr><td><i>disable</i></td><td>Disable unique auto-configuration address.</td></tr></table>	Option	Description	<i>enable</i>	Enable unique auto-configuration address.	<i>disable</i>	Disable unique auto-configuration address.			
Option	Description									
<i>enable</i>	Enable unique auto-configuration address.									
<i>disable</i>	Disable unique auto-configuration address.									
interface-identifier	IPv6 interface identifier.	ipv6-address	Not Specified	::						
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.									
ip6-delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15							
ip6-subnet	Subnet to routing prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xx x.	ipv6-prefix	Not Specified	::/0						
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.									

Parameter	Description	Type	Size	Default								
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.											
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-ip	DHCPv6 relay IP address.	user	Not Specified									
dhcp6-relay-source-ip	IPv6 address used by the DHCP6 relay as its source IP.	ipv6-address	Not Specified	::								
dhcp6-relay-interface-id	DHCP6 relay interface ID.	string	Maximum length: 64									
dhcp6-client-options	DHCPv6 client options.	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-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.											

Parameter	Description	Type	Size	Default						
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.									
cli-conn6-status	CLI IPv6 connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0						

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
prefix	IPv6 prefix.	ipv6-network	Not Specified	::/0
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the autonomous flag.		
	<i>disable</i>	Disable the autonomous flag.		
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.		

Parameter	Description	Type	Size	Default
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	604800
rdnss	Recursive DNS server option.	user	Not Specified	
dnssl <domain>	DNS search list option. Domain name.	string	Maximum length: 79	

config ip6-delegated-prefix-list

Parameter	Description	Type	Size	Default						
prefix-id	Prefix ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15							
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0						
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the autonomous flag.</td></tr><tr><td><i>disable</i></td><td>Disable the autonomous flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the autonomous flag.	<i>disable</i>	Disable the autonomous flag.			
Option	Description									
<i>enable</i>	Enable the autonomous flag.									
<i>disable</i>	Disable the autonomous flag.									
onlink-flag	Enable/disable the onlink flag.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the onlink flag.</td></tr><tr><td><i>disable</i></td><td>Disable the onlink flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the onlink flag.	<i>disable</i>	Disable the onlink flag.			
Option	Description									
<i>enable</i>	Enable the onlink flag.									
<i>disable</i>	Disable the onlink flag.									

Parameter	Description	Type	Size	Default
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified	::/0
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.		
rdnss	Recursive DNS server option.	user	Not Specified	

config dhcp6-iapd-list

Parameter	Description	Type	Size	Default
iaid	Identity association identifier.	integer	Minimum value: 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 Maximum value: 4294967295	604800
prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000

config system ipam

Configure IP address management services.

```
config system ipam
  Description: Configure IP address management services.
  set status [enable|disable]
  set server-type {option}
  set automatic-conflict-resolution [disable|enable]
```

```

set require-subnet-size-match [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}
        set subnet {ipv4-classnet}
        config exclude
            Description: Configure pool exclude subnets.
            edit <ID>
                set exclude-subnet {ipv4-classnet}
            next
        end
    next
end
config rules
    Description: Configure IPAM allocation rules.
    edit <name>
        set description {string}
        set device <name1>, <name2>, ...
        set interface <name1>, <name2>, ...
        set role [any|lan|...]
        set pool <name1>, <name2>, ...
        set dhcp [enable|disable]
    next
end
end

```

config system ipam

Parameter	Description	Type	Size	Default
status	Enable/disable IP address management services.	option	-	disable
	Option	Description		
	enable	Enable integration with IP address management services.		
	disable	Disable integration with IP address management services.		
server-type	Configure the type of IPAM server to use.	option	-	fabric-root
	Option	Description		
	fabric-root	Use the IPAM server running on the Security Fabric root.		

Parameter	Description	Type	Size	Default
automatic-conflict-resolution	Enable/disable automatic conflict resolution.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable automatic conflict resolution.		
	<i>enable</i>	Enable automatic conflict resolution.		
require-subnet-size-match	Enable/disable reassignment of subnets to make requested and actual sizes match.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable requiring subnet sizes to match.		
	<i>enable</i>	Enable requiring subnet sizes to match.		
manage-lan-addresses	Enable/disable default management of LAN interface addresses.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable LAN interface address management by default.		
	<i>enable</i>	Enable LAN interface address management by default.		
manage-lan-extension-addresses	Enable/disable default management of FortiExtender LAN extension interface addresses.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable FortiExtender LAN extension interface address management by default.		
	<i>enable</i>	Enable FortiExtender LAN extension interface address management by default.		
manage-ssid-addresses	Enable/disable default management of FortiAP SSID addresses.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable FortiAP SSID address management by default.		
	<i>enable</i>	Enable FortiAP SSID address management by default.		

config pools

Parameter	Description	Type	Size	Default
name	IPAM pool name.	string	Maximum length: 79	
description	Description.	string	Maximum length: 127	
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
name	IPAM rule name.	string	Maximum length: 79	
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	
interface <name>	Configure name or wildcard of interface to match. Interface name or wildcard.	string	Maximum length: 79	
role	Configure role of interface to match.	option	-	any
		Option	Description	
		any	Match any interface role.	
		lan	Match interface role lan.	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wan</i>	Match interface role wan.		
	<i>dmz</i>	Match interface role dmz.		
	<i>undefined</i>	Match interface role undefined.		
pool <name>	Configure name of IPAM pool to use. IPAM pool name.	string	Maximum length: 79	
dhcp	Enable/disable DHCP server for matching IPAM interfaces.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DHCP server on matched IPAM interface.		
	<i>disable</i>	Disable DHCP server on matched IPAM interface.		

config system ips

Configure IPS system settings.

```
config system ips
    Description: Configure IPS system settings.
    set signature-hold-time {user}
    set override-signature-hold-by-id [enable|disable]
end
```

config system ips

Parameter	Description	Type	Size	Default
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h> (day range: 0 - 7, hour range: 0 - 23, max hold time: 7d0h, default hold time: 0d0h).	user	Not Specified	0h
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.		

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 status [enable|disable]
    set ipv6-capability [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
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this DNS server for IPS URL filter DNS queries.		
	<i>disable</i>	Disable this DNS server for IPS URL filter DNS queries.		
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

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	
		enable	Enable setting.	
		disable	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:xx xx).	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 ip-conflict status

List interface names and IP addresses in conflict.

```
config system ip-conflict status
    Description: List interface names and IP addresses in conflict.
end
```

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 srcintf {string}
        set server-config [default|individual]
        set server-type [static|dynamic]
        set server <address1>, <address2>, ...
        set protocol {option1}, {option2}, ...
        set port {integer}
        set gateway-ip {ipv4-address-any}
        set gateway-ip6 {ipv6-address}
        set route <subnet1>, <subnet2>, ...
        set source-ip {ipv4-address-any}
        set source-ip6 {ipv6-address}
        set http-get {string}
        set http-agent {string}
        set http-match {string}
        set interval {integer}
        set probe-timeout {integer}
        set failtime {integer}
        set recoverytime {integer}
        set probe-count {integer}
        set security-mode [none|authentication]
        set password {password}
        set packet-size {integer}
        set ha-priority {integer}
        set fail-weight {integer}
        set update-cascade-interface [enable|disable]
        set update-static-route [enable|disable]
        set update-policy-route [enable|disable]
        set status [enable|disable]
        set diffservcode {user}
        set class-id {integer}
        set service-detection [enable|disable]
    config server-list
        Description: Servers for link-monitor to monitor.
```

```

        edit <id>
            set dst {string}
            set protocol {option1}, {option2}, ...
            set port {integer}
            set weight {integer}
        next
    end
next
end

```

config system link-monitor

Parameter	Description	Type	Size	Default
name	Link monitor name.	string	Maximum length: 35	
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option Description			
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15	
server-config	Mode of server configuration.	option	-	default
	Option Description			
	<i>default</i>	All servers share the same attributes.		
	<i>individual</i>	Some attributes can be specified for individual servers.		
server-type	Server type (static or dynamic).	option	-	static
	Option Description			
	<i>static</i>	Static servers.		
	<i>dynamic</i>	Dynamic servers.		
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79	
protocol	Protocols used to monitor the server.	option	-	ping

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING link monitor.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo link monitor.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo link monitor.</td></tr><tr><td><i>http</i></td><td>HTTP-GET link monitor.</td></tr><tr><td><i>https</i></td><td>HTTPS-GET link monitor.</td></tr><tr><td><i>twamp</i></td><td>TWAMP link monitor.</td></tr></table>	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.			
	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.																	
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0														
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	::														
route <subnet>	Subnet to monitor. IP and netmask (x.x.x.x/y).	string	Maximum length: 79															
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	::														
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-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/														
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														

Parameter	Description	Type	Size	Default						
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						
failtime	Number of retry attempts before the server is considered down (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600	5						
recoverytime	Number of successful responses received before server is considered recovered (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600	5						
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						
security-mode	Twamp controller security mode.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Unauthenticated mode.</td></tr><tr><td><i>authentication</i></td><td>Authenticated mode.</td></tr></table>				Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.
Option	Description									
<i>none</i>	Unauthenticated mode.									
<i>authentication</i>	Authenticated mode.									
password	TWAMP controller password in authentication mode.	password	Not Specified							
packet-size	Packet size of a TWAMP test session (124/158 - 1024).	integer	Minimum value: 0 Maximum value: 65535	124						
ha-priority	HA election priority (1 - 50).	integer	Minimum value: 1 Maximum value: 50	1						
fail-weight	Threshold weight to trigger link failure alert.	integer	Minimum value: 0 Maximum value: 255	0						
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable						

Parameter	Description	Type	Size	Default
	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.		
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.		
status	Enable/disable this link monitor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this link monitor.		
	<i>disable</i>	Disable this link monitor.		
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified	
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
service-detection	Only use monitor to read quality values. If enabled, static routes and cascade interfaces will not be updated.	option	-	disable
	Option	Description		
	<i>enable</i>	Only use monitor for service-detection.		
	<i>disable</i>	Monitor will update routes/interfaces on link failure.		

config server-list

Parameter	Description	Type	Size	Default														
id	Server ID.	integer	Minimum value: 1 Maximum value: 32	0														
dst	IP address of the server to be monitored.	string	Maximum length: 64															
protocol	Protocols used to monitor the server.	option	-	ping														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING link monitor.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo link monitor.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo link monitor.</td></tr><tr><td><i>http</i></td><td>HTTP-GET link monitor.</td></tr><tr><td><i>https</i></td><td>HTTPS-GET link monitor.</td></tr><tr><td><i>twamp</i></td><td>TWAMP link monitor.</td></tr></table>				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.
	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.																	
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0														
weight	Weight of the monitor to this dst (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0														

config system management-tunnel

Management tunnel configuration.

```
config system management-tunnel
  Description: Management tunnel configuration.
  set status [enable|disable]
  set allow-config-restore [enable|disable]
  set allow-push-configuration [enable|disable]
  set allow-push-firmware [enable|disable]
  set allow-collect-statistics [enable|disable]
  set authorized-manager-only [enable|disable]
  set serial-number {user}
end
```


config system management-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable FGFM tunnel.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable management tunnel.		
	<i>disable</i>	Disable management tunnel.		
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
	Option	Description		
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		
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.		
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable restriction of authorized manager only.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable restriction of authorized manager only.		
serial-number	Serial number.	user	Not Specified	

config system mgmt-csum

System checksum for FortiManager use only.

```
config system mgmt-csum
    Description: System checksum for FortiManager use only.
end
```

config system nethsm

Configure system nethsm.

```
config system nethsm
    Description: Configure system nethsm.
    set status [enable|disable]
    set vendor [safenet|primus]
    set interface {string}
    set receivetimeout {integer}
    config servers
        Description: NetHSM server list.
        edit <name>
            set server {string}
            set port {integer}
            set server-cert {user}
            set htl [enable|disable]
        next
    end
    config slots
        Description: NetHSM slot list.
        edit <name>
            set id {integer}
            set password {password}
            set for-ha [yes|no]
        next
    end
    set ha [enable|disable]
    set ha-status-pulling-interval {integer}
    config hgroups
        Description: NetHSM HA group list.
```

```

    edit <name>
        set member <name1>, <name2>, ...
    next
end
set rsa-mech-remap [enable|disable]
set primus-cfg {user}
set secret-content {password_aes256}
config partitions
    Description: Set Hardware Security Module partition information.
    edit <name>
        set slot-id {integer}
        set pkcs11-pin {password}
    next
end
end

```

config system nethsm

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable system network HSM.		
	<i>disable</i>	Disable system network HSM.		
vendor	Vendor.	option	-	safenet
	Option	Description		
	<i>safenet</i>	SafeNet HSM.		
	<i>primus</i>	Securosys Primus HSM.		
interface	Outgoing interface	string	Maximum length: 15	
receivetimeout	Receive timeout, specified in ms (default=20000).	integer	Minimum value: 0 Maximum value: 4294967295	20000
ha	HA option (default=disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HA.		
	<i>disable</i>	Disable HA.		

Parameter	Description	Type	Size	Default						
ha-status-pulling-interval	Interval to pull HA status in minutes (default=1).	integer	Minimum value: 0 Maximum value: 60	1						
rsa-mech-remap	RSA Mechanism Remap option (default=disable). Enable it if Luna server is running in FIPS mode and firmware version is 6.22.* or greater.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RSA Mechanism Remap.</td></tr><tr><td><i>disable</i></td><td>Disable RSA Mechanism Remap.</td></tr></table>	Option	Description	<i>enable</i>	Enable RSA Mechanism Remap.	<i>disable</i>	Disable RSA Mechanism Remap.			
Option	Description									
<i>enable</i>	Enable RSA Mechanism Remap.									
<i>disable</i>	Disable RSA Mechanism Remap.									
primus-cfg	Set primus.cfg file content	user	Not Specified							
secret-content	Set secret content	password_ aes256	Not Specified							

config servers

Parameter	Description	Type	Size	Default						
name	NetHSM server name.	string	Maximum length: 35							
server	{<name_str ip_str>} NetHSM server domain name or IP.	string	Maximum length: 63							
port	NetHSM server port (default=1792).	integer	Minimum value: 1 Maximum value: 65535	1792						
server-cert	NetHSM server certificate.	user	Not Specified							
htl	HTL option (default=disable).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTL.</td></tr><tr><td><i>disable</i></td><td>Disable HTL.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTL.	<i>disable</i>	Disable HTL.			
Option	Description									
<i>enable</i>	Enable HTL.									
<i>disable</i>	Disable HTL.									

config slots

Parameter	Description	Type	Size	Default
name	NetHSM slot name.	string	Maximum length: 35	
id	NetHSM slot ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0
password	NetHSM slot access password.	password	Not Specified	
for-ha	HA option.	option	-	no
	Option	Description		
	yes	HA slot.		
	no	Regular slot.		

config hagroups

Parameter	Description	Type	Size	Default
name	NetHSM HA group name.	string	Maximum length: 35	
member <name>	HA group members. NetHSM HA group member (slot names).	string	Maximum length: 79	

config partitions

Parameter	Description	Type	Size	Default
name	Name of the Hardware Security Module partition.	string	Maximum length: 35	
slot-id	Slot ID number of the Hardware Security Module partition.	integer	Minimum value: 0 Maximum value: 4294967295	0
pkcs11-pin	PKCS#11 PIN for the Hardware Security Module partition.	password	Not Specified	

config system network-visibility

Configure network visibility settings.

```
config system network-visibility
  Description: Configure network visibility settings.
  set destination-visibility [disable|enable]
  set source-location [disable|enable]
  set destination-hostname-visibility [disable|enable]
  set hostname-ttl {integer}
  set hostname-limit {integer}
  set destination-location [disable|enable]
end
```

config system network-visibility

Parameter	Description	Type	Size	Default						
destination-visibility	Enable/disable logging of destination visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of destination visibility.</td></tr><tr><td><i>enable</i></td><td>Enable logging of destination visibility.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of destination visibility.	<i>enable</i>	Enable logging of destination visibility.			
Option	Description									
<i>disable</i>	Disable logging of destination visibility.									
<i>enable</i>	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><i>disable</i></td><td>Disable logging of source geographical location visibility.</td></tr><tr><td><i>enable</i></td><td>Enable logging of source geographical location visibility.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of source geographical location visibility.	<i>enable</i>	Enable logging of source geographical location visibility.			
Option	Description									
<i>disable</i>	Disable logging of source geographical location visibility.									
<i>enable</i>	Enable logging of source geographical location visibility.									
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of destination hostname visibility.</td></tr><tr><td><i>enable</i></td><td>Enable logging of destination hostname visibility.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of destination hostname visibility.	<i>enable</i>	Enable logging of destination hostname visibility.			
Option	Description									
<i>disable</i>	Disable logging of destination hostname visibility.									
<i>enable</i>	Enable logging of destination hostname visibility.									
hostname-ttl	TTL of hostname table entries (60 - 86400).	integer	Minimum value: 60 Maximum value: 86400	86400						

Parameter	Description	Type	Size	Default
hostname-limit	Limit of the number of hostname table entries (0 - 50000).	integer	Minimum value: 0 Maximum value: 50000	5000
destination-location	Enable/disable logging of destination geographical location visibility.	option	-	enable
		Option	Description	
		<i>disable</i>	Disable logging of destination geographical location visibility.	
		<i>enable</i>	Enable logging of destination geographical location visibility.	

config system ntp

Configure system NTP information.

```

config system ntp
  Description: Configure system NTP information.
  set ntpsync [enable|disable]
  set type [fortiguard|custom]
  set syncinterval {integer}
  config ntpserver
    Description: Configure the FortiProxy to connect to any available third-party NTP server.
    edit <id>
      set server {string}
      set ntpv3 [enable|disable]
      set authentication [enable|disable]
      set key-type [MD5|SHA1|...]
      set key {password}
      set key-id {integer}
      set ip-type [IPv6|IPv4|...]
      set interface-select-method [auto|specify]
      set interface {string}
    next
  end
  set source-ip {ipv4-address}
  set source-ip6 {ipv6-address}
  set server-mode [enable|disable]
  set authentication [enable|disable]
  set key-type [MD5|SHA1|...]
  set key {password}
  set key-id {integer}
  set interface <interface-name1>, <interface-name2>, ...
end

```

config system ntp

Parameter	Description	Type	Size	Default
ntpsync	Enable/disable setting the FortiProxy system time by synchronizing with an NTP Server.	option	-	disable
	Option Description			
	enable	Enable synchronization with NTP Server.		
	disable	Disable synchronization with NTP Server.		
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-	fortiguard
	Option Description			
	fortiguard	Use the FortiGuard NTP server.		
	custom	Use any other available NTP server.		
syncinterval	NTP synchronization interval (1 - 1440 min).	integer	Minimum value: 1 Maximum value: 1440	60
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	::
server-mode	Enable/disable FortiProxy NTP Server Mode. Your FortiProxy becomes an NTP server for other devices on your network. The FortiProxy relays NTP requests to its configured NTP server.	option	-	disable
	Option Description			
	enable	Enable FortiProxy NTP Server Mode.		
	disable	Disable FortiProxy NTP Server Mode.		
authentication	Enable/disable authentication.	option	-	disable
	Option Description			
	enable	Enable authentication.		
	disable	Disable authentication.		

Parameter	Description	Type	Size	Default								
key-type	Key type for authentication (MD5, SHA1, SHA256).	option	-	MD5								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>MD5</td><td>Use MD5 to authenticate the message.</td></tr><tr><td>SHA1</td><td>Use SHA1 to authenticate the message.</td></tr><tr><td>SHA256</td><td>Use SHA256 to authenticate the message.</td></tr></table>				Option	Description	MD5	Use MD5 to authenticate the message.	SHA1	Use SHA1 to authenticate the message.	SHA256	Use SHA256 to authenticate the message.
	Option	Description										
	MD5	Use MD5 to authenticate the message.										
	SHA1	Use SHA1 to authenticate the message.										
SHA256	Use SHA256 to authenticate the message.											
key	Key for authentication.	password	Not Specified									
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0								
interface <interface-name>	FortiProxy interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79									

config ntpserver

Parameter	Description	Type	Size	Default						
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
server	IP address or hostname of the NTP Server.	string	Maximum length: 63							
ntpv3	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).									
authentication	Enable/disable authentication.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable authentication.		
	<i>disable</i>	Disable authentication.		
key-type	Select NTP authentication type.	option	-	MD5
	Option	Description		
	<i>MD5</i>	Enable MD5(NTPv3) authentication.		
	<i>SHA1</i>	Enable SHA1(NTPv4) authentication.		
	<i>SHA256</i>	Enable SHA256(NTPv4) authentication.		
key	Key for MD5(NTPv3)/SHA1 (NTPv4)/SHA256(NTPv4) authentication.	password	Not Specified	
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-type	Choose to connect to IPv4 or/and IPv6 NTP server.	option	-	Both
	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.		
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system object-tagging

Configure object tagging.

```

config system object-tagging
  Description: Configure object tagging.
  edit <category>
    set address [disable|mandatory|...]
    set device [disable|mandatory|...]
    set interface [disable|mandatory|...]
    set multiple [enable|disable]
    set color {integer}
    set tags <name1>, <name2>, ...
  next
end

```

config system object-tagging

Parameter	Description	Type	Size	Default
category	Tag Category.	string	Maximum length: 63	
address	Address.	option	-	optional
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
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.		
multiple	Allow multiple tag selection.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable multi-tagging.		
	<i>disable</i>	Disable multi-tagging.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
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 status [enable|disable]
    set apply-to {option1}, {option2}, ...
    set minimum-length {integer}
    set min-lower-case-letter {integer}
    set min-upper-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-change-characters {integer}
    set expire-status [enable|disable]
    set expire-day {integer}
    set reuse-password [enable|disable]
    set login-lockout-upon-downgrade [enable|disable]
    set password-history {integer}
end

```

config system password-policy

Parameter	Description	Type	Size	Default
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.			
	Option	Description								
	<i>enable</i>	Enable password policy.								
<i>disable</i>	Disable password policy.									
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.									
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase 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						
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-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						
expire-status	Enable/disable password expiration.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Passwords expire after expire-day days.		
	<i>disable</i>	Passwords do not expire.		
expire-day	Number of days after which passwords expire (1 - 999 days, default = 90).	integer	Minimum value: 1 Maximum value: 999	90
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable
	Option	Description		
	<i>enable</i>	Administrators are allowed to reuse the same password.		
	<i>disable</i>	Administrators must create a new password.		
login-lockout-upon-downgrade	Enable/disable administrative user login lockout upon downgrade (default = disable). If enabled, downgrading the FortiOS firmware to a lower version where safer passwords are unsupported will lock out administrative users.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable administrative user login lockout upon downgrade.		
	<i>disable</i>	Disable administrative user login lockout upon downgrade.		
password-history	Number of previous passwords that cannot be reused.	integer	Minimum value: 2 Maximum value: 20	2

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 status [enable|disable]
  set apply-to {option1}, {option2}, ...
  set minimum-length {integer}
  set min-lower-case-letter {integer}
```

```

set min-upper-case-letter {integer}
set min-non-alphanumeric {integer}
set min-number {integer}
set min-change-characters {integer}
set expire-status [enable|disable]
set expire-day {integer}
set reuse-password [enable|disable]
set password-history {integer}
end

```

config system password-policy-guest-admin

Parameter	Description	Type	Size	Default						
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><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.			
Option	Description									
<i>enable</i>	Enable password policy.									
<i>disable</i>	Disable password policy.									
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><i>guest-admin-password</i></td><td>Apply to guest administrator password.</td></tr></table>	Option	Description	<i>guest-admin-password</i>	Apply to guest administrator password.					
Option	Description									
<i>guest-admin-password</i>	Apply to guest administrator password.									
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase 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						
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-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						
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.									
expire-day	Number of days after which passwords expire (1 - 999 days, default = 90).	integer	Minimum value: 1 Maximum value: 999	90						
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><i>enable</i></td><td>Administrators are allowed to reuse the same password.</td></tr><tr><td><i>disable</i></td><td>Administrators must create a new password.</td></tr></table>				Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.
Option	Description									
<i>enable</i>	Administrators are allowed to reuse the same password.									
<i>disable</i>	Administrators must create a new password.									
password-history	Number of previous passwords that cannot be reused.	integer	Minimum value: 2 Maximum value: 20	2						

config system performance status

System performance status.


```
config system performance status
    Description: System performance status.
end
```

config system performance top

Display information about the top CPU processes.

```
config system performance top
    Description: Display information about the top CPU processes.
    set <delay> {string}
end
```

config system performance top

Parameter	Description	Type	Size	Default
<delay>	Delay in seconds (default 5).	string	Maximum length: -	

config system probe-response

Configure system probe response.

```
config system probe-response
    Description: Configure system probe response.
    set port {integer}
    set http-probe-value {string}
    set ttl-mode [reinit|decrease|...]
    set mode [none|http-probe|...]
    set security-mode [none|authentication]
    set password {password}
    set timeout {integer}
end
```

config system probe-response

Parameter	Description	Type	Size	Default								
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535	8008								
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024	OK								
ttl-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.											
mode	SLA response mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable probe.</td></tr><tr><td><i>http-probe</i></td><td>HTTP probe.</td></tr><tr><td><i>twamp</i></td><td>Two way active measurement protocol.</td></tr></table>	Option	Description	<i>none</i>	Disable probe.	<i>http-probe</i>	HTTP probe.	<i>twamp</i>	Two way active measurement protocol.			
Option	Description											
<i>none</i>	Disable probe.											
<i>http-probe</i>	HTTP probe.											
<i>twamp</i>	Two way active measurement protocol.											
security-mode	TWAMP responder security mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Unauthenticated mode.</td></tr><tr><td><i>authentication</i></td><td>Authenticated mode.</td></tr></table>	Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.					
Option	Description											
<i>none</i>	Unauthenticated mode.											
<i>authentication</i>	Authenticated mode.											
password	TWAMP responder password in authentication mode.	password	Not Specified									
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600	300								

config system proxy-arp

Configure proxy-ARP.

```
config system proxy-arp
  Description: Configure proxy-ARP.
  edit <id>
    set interface {string}
    set ip {ipv4-address}
    set end-ip {ipv4-address}
  next
end
```

config system proxy-arp

Parameter	Description	Type	Size	Default
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
end-ip	End IP of IP range 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 status [enable|disable]
  set mode [multicast|hybrid]
  set delay-mechanism [E2E|P2P]
  set request-interval {integer}
  set interface {string}
  set server-mode [enable|disable]
  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 server-interface-name {string}
        set delay-mechanism [E2E|P2P]
    next
end
end

```

config system ptp

Parameter	Description	Type	Size	Default						
status	Enable/disable setting the FortiProxy 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.									
mode	Multicast transmission or hybrid transmission.	option	-	multicast						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multicast</i></td><td>Send PTP packets with multicast.</td></tr><tr><td><i>hybrid</i></td><td>Send PTP packets with unicast and multicast.</td></tr></table>	Option	Description	<i>multicast</i>	Send PTP packets with multicast.	<i>hybrid</i>	Send PTP packets with unicast and multicast.			
Option	Description									
<i>multicast</i>	Send PTP packets with multicast.									
<i>hybrid</i>	Send PTP packets with unicast and multicast.									
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><i>E2E</i></td><td>End to end delay detection.</td></tr><tr><td><i>P2P</i></td><td>Peer to peer delay detection.</td></tr></table>	Option	Description	<i>E2E</i>	End to end delay detection.	<i>P2P</i>	Peer to peer delay detection.			
Option	Description									
<i>E2E</i>	End to end delay detection.									
<i>P2P</i>	Peer to peer delay detection.									
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						
interface	PTP client will reply through this interface.	string	Maximum length: 15							
server-mode	Enable/disable FortiGate PTP server mode. Your FortiGate becomes an PTP server for other devices on your network.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FortiGate PTP server mode.		
	<i>disable</i>	Disable FortiGate PTP server mode.		

config server-interface

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-interface-name	Interface name.	string	Maximum length: 15	
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E
	Option	Description		
	<i>E2E</i>	End to end delay detection.		
	<i>P2P</i>	Peer to peer delay detection.		

config system replacemsg admin

Replacement messages.

```

config system replacemsg admin
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end

```

config system replacemsg admin

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg alertmail

Replacement messages.

```
config system replacemsg alertmail
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg alertmail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg auth

Replacement messages.

```
config system replacemsg auth
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg auth

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg automation

Replacement messages.

```
config system replacemsg automation
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```


config system replacemsg automation

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg custom-message

Replacement messages.

```
config system replacemsg custom-message
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg custom-message

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option Description			
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option Description			
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg fortiguard-wf

Replacement messages.

```
config system replacemsg fortiguard-wf
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg ftp

Replacement messages.

```
config system replacemsg ftp
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg ftp

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg http

Replacement messages.

```
config system replacemsg http
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg http

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg icap

Replacement messages.

```
config system replacemsg icap
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg icap

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg mail

Replacement messages.

```
config system replacemsg mail
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg mail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg nac-quar

Replacement messages.

```
config system replacemsg nac-quar
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg nac-quar

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option Description			
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option Description			
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg spam

Replacement messages.

```
config system replacemsg spam
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```


config system replacemsg spam

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg sslvpn

Replacement messages.

```
config system replacemsg sslvpn
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg sslvpn

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg traffic-quota

Replacement messages.

```
config system replacemsg traffic-quota
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg traffic-quota

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg utm

Replacement messages.

```
config system replacemsg utm
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg utm

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg webproxy

Replacement messages.

```
config system replacemsg webproxy
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg webproxy

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg-group

Configure replacement message groups.

```
config system replacemsg-group
  Description: Configure replacement message groups.
  edit <name>
    set comment {var-string}
    set group-type [default|utm|...]
    config mail
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
      next
    end
  config http
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
```

```

        set header [none|http|...]
        set format [none|text|...]
    next
end
config webproxy
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config ftp
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config fortiguard-wf
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config spam
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config alertmail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config admin
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end

```

```

config auth
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config sslvpn
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config nac-quar
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config traffic-quota
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config utm
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config custom-message
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config icap
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}

```

```

        set header [none|http|...]
        set format [none|text|...]
    next
end
config automation
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
next
end

```

config system replacemsg-group

Parameter	Description	Type	Size	Default								
name	Group name.	string	Maximum length: 35									
comment	Comment.	var-string	Maximum length: 255									
group-type	Group type.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Per-vdom replacement messages.</td></tr><tr><td><i>utm</i></td><td>For use with UTM settings in firewall policies.</td></tr><tr><td><i>auth</i></td><td>For use with authentication pages in firewall policies.</td></tr></table>				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.
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.											

config mail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config http

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config webproxy

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option Description			
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option Description			
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config ftp

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
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.											
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.		

config fortiguard-wf

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config spam

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config alertmail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config admin

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
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.											
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.											

config auth

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
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.											
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.		

config sslvpn

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config nac-quar

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config traffic-quota

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config utm

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option Description			
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option Description			
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config custom-message

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
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.											
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.		

config icap

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config automation

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg-image

Configure replacement message images.

```
config system replacemsg-image
  Description: Configure replacement message images.
  edit <name>
    set image-type [gif|jpg|...]
    set image-base64 {var-string}
  next
end
```

config system replacemsg-image

Parameter	Description	Type	Size	Default
name	Image name.	string	Maximum length: 23	
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.		

Parameter	Description	Type	Size	Default
image-base64	Image data.	var-string	Maximum length: 32768	

config system resource-limits

Configure resource limits.

```

config system resource-limits
    Description: Configure resource limits.
    set ipsec-phase1-interface {integer}
    set ipsec-phase2-interface {integer}
    set firewall-policy {integer}
    set firewall-address {integer}
    set firewall-addrgrp {integer}
    set custom-service {integer}
    set service-group {integer}
    set onetime-schedule {integer}
    set recurring-schedule {integer}
    set user {integer}
    set user-group {integer}
    set proxy {integer}
    set log-disk-quota {integer}
end

```

config system resource-limits

Parameter	Description	Type	Size	Default
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface 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	
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
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	
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295	
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295	
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
recurring-schedule	Maximum number of firewall recurring schedules.	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	

Parameter	Description	Type	Size	Default
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295	
log-disk-quota	Log disk quota in megabytes (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0

config system saml

Global settings for SAML authentication.

```

config system saml
  Description: Global settings for SAML authentication.
  set status [enable|disable]
  set role [identity-provider|service-provider]
  set default-login-page [normal|sso]
  set default-profile {string}
  set cert {string}
  set binding-protocol [post|redirect]
  set portal-url {string}
  set entity-id {string}
  set single-sign-on-url {string}
  set single-logout-url {string}
  set idp-entity-id {string}
  set idp-single-sign-on-url {string}
  set idp-single-logout-url {string}
  set idp-cert {string}
  set server-address {string}
  set tolerance {integer}
  set life {integer}
  config service-providers
    Description: Authorized service providers.
    edit <name>
      set prefix {string}
      set sp-binding-protocol [post|redirect]
      set sp-cert {string}
      set sp-entity-id {string}
      set sp-single-sign-on-url {string}
      set sp-single-logout-url {string}
      set sp-portal-url {string}
      set idp-entity-id {string}
      set idp-single-sign-on-url {string}
      set idp-single-logout-url {string}

```

```

        config assertion-attributes
            Description: Customized SAML attributes to send along with assertion.
            edit <name>
                set type [username|email|...]
            next
        end
    next
end
end
end

```

config system saml

Parameter	Description	Type	Size	Default
status	Enable/disable SAML authentication (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SAML authentication.		
	<i>disable</i>	Disable SAML authentication.		
role	SAML role.	option	-	service-provider
	Option	Description		
	<i>identity-provider</i>	Identity Provider.		
	<i>service-provider</i>	Service Provider.		
default-login-page	Choose default login page.	option	-	normal
	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	
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
binding-protocol	IdP Binding protocol.	option	-	redirect

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>post</i>	HTTP POST binding.		
	<i>redirect</i>	HTTP Redirect binding.		
portal-url	SP portal URL.	string	Maximum length: 255	
entity-id	SP entity ID.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
single-logout-url	SP single logout URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	
idp-cert	IDP certificate name.	string	Maximum length: 35	
server-address	Server address.	string	Maximum length: 63	
tolerance	Tolerance to the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	5
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	30

config service-providers

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

Parameter	Description	Type	Size	Default
prefix	Prefix.	string	Maximum length: 35	
sp-binding-protocol	SP binding protocol.	option	-	post
	Option	Description		
	<i>post</i>	HTTP POST binding.		
	<i>redirect</i>	HTTP Redirect binding.		
sp-cert	SP certificate name.	string	Maximum length: 35	
sp-entity-id	SP entity ID.	string	Maximum length: 255	
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255	
sp-portal-url	SP portal URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	

config assertion-attributes

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Type.	option	-	username
	Option	Description		
	username	User Name.		
	email	Email Address.		
	profile-name	Profile Name.		

config system sdn-connector

Configure connection to SDN Connector.

```
config system sdn-connector
  Description: Configure connection to SDN Connector.
  edit <name>
    set status [disable|enable]
    set type [aci|alicloud|...]
    set proxy {string}
    set use-metadata-iam [disable|enable]
    set ha-status [disable|enable]
    set verify-certificate [disable|enable]
    set server {string}
    set server-list <ip1>, <ip2>, ...
    set server-port {integer}
    set username {string}
    set password {password_aes256}
    set vcenter-server {string}
    set vcenter-username {string}
    set vcenter-password {password_aes256}
    set access-key {string}
    set secret-key {password}
    set region {string}
    set vpc-id {string}
    set alt-resource-ip [disable|enable]
  config external-account-list
    Description: Configure AWS external account list.
    edit <role-arn>
      set external-id {string}
      set region-list <region1>, <region2>, ...
    next
  end
  set tenant-id {string}
  set client-id {string}
  set client-secret {password}
  set subscription-id {string}
  set resource-group {string}
  set login-endpoint {string}
  set resource-url {string}
  set azure-region [global|china|...]
  config nic
    Description: Configure Azure network interface.
    edit <name>
      set peer-nic {string}
    config ip
      Description: Configure IP configuration.
      edit <name>
        set private-ip {string}
        set public-ip {string}
        set resource-group {string}
```

```

        next
    end
next
end
config route-table
    Description: Configure Azure route table.
    edit <name>
        set subscription-id {string}
        set resource-group {string}
        config route
            Description: Configure Azure route.
            edit <name>
                set next-hop {string}
            next
        end
    next
end
set user-id {string}
config compartment-list
    Description: Configure OCI compartment list.
    edit <compartment-id>
        next
    end
config oci-region-list
    Description: Configure OCI region list.
    edit <region>
        next
    end
set oci-region-type [commercial|government]
set oci-cert {string}
set oci-fingerprint {string}
config external-ip
    Description: Configure GCP external IP.
    edit <name>
        next
    end
config route
    Description: Configure GCP route.
    edit <name>
        next
    end
config gcp-project-list
    Description: Configure GCP project list.
    edit <id>
        set gcp-zone-list <name1>, <name2>, ...
    next
end
config forwarding-rule
    Description: Configure GCP forwarding rule.
    edit <rule-name>
        set target {string}
    next

```

```

end
set service-account {string}
set private-key {user}
set secret-token {user}
set domain {string}
set group-name {string}
set server-cert {string}
set server-ca-cert {string}
set api-key {password}
set compute-generation {integer}
set ibm-region [dallas|washington-dc|...]
set update-interval {integer}
next
end

```

config system sdn-connector

Parameter	Description	Type	Size	Default
name	SDN connector name.	string	Maximum length: 35	
status	Enable/disable connection to the remote SDN connector.	option	-	enable
	Option Description			
	disable	Disable connection to this SDN Connector.		
	enable	Enable connection to this SDN Connector.		
type	Type of SDN connector.	option	-	aws
	Option Description			
	aci	Application Centric Infrastructure (ACI).		
	alicloud	AliCloud Service (ACS).		
	aws	Amazon Web Services (AWS).		
	azure	Microsoft Azure.		
	gcp	Google Cloud Platform (GCP).		
	nsx	VMware NSX.		
	nuage	Nuage VSP.		
	oci	Oracle Cloud Infrastructure.		
	openstack	OpenStack.		
	kubernetes	Kubernetes.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></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>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>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.																	
proxy	SDN proxy.	string	Maximum length: 35															
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.																	
ha-status	Enable/disable use for FortiProxy HA service.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use for FortiProxy HA service.</td></tr><tr><td><i>enable</i></td><td>Enable use for FortiProxy HA service.</td></tr></table>	Option	Description	<i>disable</i>	Disable use for FortiProxy HA service.	<i>enable</i>	Enable use for FortiProxy HA service.											
	Option	Description																
	<i>disable</i>	Disable use for FortiProxy HA service.																
<i>enable</i>	Enable use for FortiProxy HA service.																	
verify-certificate	Enable/disable server certificate verification.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable server certificate verification.</td></tr><tr><td><i>enable</i></td><td>Enable server certificate verification.</td></tr></table>	Option	Description	<i>disable</i>	Disable server certificate verification.	<i>enable</i>	Enable server certificate verification.											
	Option	Description																
	<i>disable</i>	Disable server certificate verification.																
<i>enable</i>	Enable server certificate verification.																	
server	Server address of the remote SDN connector.	string	Maximum length: 127															
server-list <ip>	Server address list of the remote SDN connector. IPv4 address.	string	Maximum length: 15															

Parameter	Description	Type	Size	Default						
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535	0						
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64							
password	Password of the remote SDN connector as login credentials.	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							
vcenter-password	vCenter server password for NSX quarantine.	password_aes256	Not Specified							
access-key	AWS / ACS access key ID.	string	Maximum length: 31							
secret-key	AWS / ACS secret access key.	password	Not Specified							
region	AWS / ACS region name.	string	Maximum length: 31							
vpc-id	AWS VPC ID.	string	Maximum length: 31							
alt-resource-ip	Enable/disable AWS alternative resource IP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable AWS alternative resource IP.</td></tr><tr><td>enable</td><td>Enable AWS alternative resource IP.</td></tr></table>				Option	Description	disable	Disable AWS alternative resource IP.	enable	Enable AWS alternative resource IP.
Option	Description									
disable	Disable AWS alternative resource IP.									
enable	Enable AWS alternative resource IP.									
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127							
client-id	Azure client ID (application ID).	string	Maximum length: 63							
client-secret	Azure client secret (application key).	password	Not Specified							
subscription-id	Azure subscription ID.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default												
resource-group	Azure resource group.	string	Maximum length: 63													
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127													
resource-url	Azure Stack resource URL.	string	Maximum length: 127													
azure-region	Azure server region.	option	-	global												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global Azure Server.</td></tr><tr><td><i>china</i></td><td>China Azure Server.</td></tr><tr><td><i>germany</i></td><td>Germany Azure Server.</td></tr><tr><td><i>usgov</i></td><td>US Government Azure Server.</td></tr><tr><td><i>local</i></td><td>Azure Stack Local Server.</td></tr></table>	Option	Description	<i>global</i>	Global Azure Server.	<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.			
Option	Description															
<i>global</i>	Global Azure Server.															
<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.															
user-id	User ID.	string	Maximum length: 127													
oci-region-type	OCI region type.	option	-	commercial												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>commercial</i></td><td>Commercial region.</td></tr><tr><td><i>government</i></td><td>Government region.</td></tr></table>	Option	Description	<i>commercial</i>	Commercial region.	<i>government</i>	Government region.									
Option	Description															
<i>commercial</i>	Commercial region.															
<i>government</i>	Government region.															
oci-cert	OCI certificate.	string	Maximum length: 63													
oci-fingerprint	OCI pubkey fingerprint.	string	Maximum length: 63													
service-account	GCP service account email.	string	Maximum length: 127													
private-key	Private key of GCP service account.	user	Not Specified													
secret-token	Secret token of Kubernetes service account.	user	Not Specified													
domain	Domain name.	string	Maximum length: 127													
group-name	Full path group name of computers.	string	Maximum length: 127													

Parameter	Description	Type	Size	Default																				
server-cert	Trust servers that contain this certificate only.	string	Maximum length: 127																					
server-ca-cert	Trust only those servers whose certificate is directly/indirectly signed by this certificate.	string	Maximum length: 127																					
api-key	IBM cloud API key or service ID API key.	password	Not Specified																					
compute-generation	Compute generation for IBM cloud infrastructure.	integer	Minimum value: 1 Maximum value: 2	2																				
ibm-region	IBM cloud region name.	option	-	dallas																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dallas</td><td>US South (Dallas) Public Endpoint.</td></tr><tr><td>washington-dc</td><td>US East (Washington DC) Public Endpoint.</td></tr><tr><td>london</td><td>United Kingdom (London) Public Endpoint.</td></tr><tr><td>frankfurt</td><td>Germany (Frankfurt) Public Endpoint.</td></tr><tr><td>sydney</td><td>Australia (Sydney) Public Endpoint.</td></tr><tr><td>tokyo</td><td>Japan (Tokyo) Public Endpoint.</td></tr><tr><td>osaka</td><td>Japan (Osaka) Public Endpoint.</td></tr><tr><td>toronto</td><td>Canada (Toronto) Public Endpoint.</td></tr><tr><td>sao-paulo</td><td>Brazil (Sao Paulo) Public Endpoint.</td></tr></table>				Option	Description	dallas	US South (Dallas) Public Endpoint.	washington-dc	US East (Washington DC) Public Endpoint.	london	United Kingdom (London) Public Endpoint.	frankfurt	Germany (Frankfurt) Public Endpoint.	sydney	Australia (Sydney) Public Endpoint.	tokyo	Japan (Tokyo) Public Endpoint.	osaka	Japan (Osaka) Public Endpoint.	toronto	Canada (Toronto) Public Endpoint.	sao-paulo	Brazil (Sao Paulo) Public Endpoint.
	Option	Description																						
	dallas	US South (Dallas) Public Endpoint.																						
	washington-dc	US East (Washington DC) Public Endpoint.																						
	london	United Kingdom (London) Public Endpoint.																						
	frankfurt	Germany (Frankfurt) Public Endpoint.																						
	sydney	Australia (Sydney) Public Endpoint.																						
	tokyo	Japan (Tokyo) Public Endpoint.																						
	osaka	Japan (Osaka) Public Endpoint.																						
	toronto	Canada (Toronto) Public Endpoint.																						
sao-paulo	Brazil (Sao Paulo) Public Endpoint.																							
update-interval	Dynamic object update interval (30 - 3600 sec, default = 60, 0 = disabled).	integer	Minimum value: 0 Maximum value: 3600	60																				

config external-account-list

Parameter	Description	Type	Size	Default
role-arn	AWS role ARN to assume.	string	Maximum length: 2047	

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	

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 route-table

Parameter	Description	Type	Size	Default
name	Route table name.	string	Maximum length: 63	
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63	
resource-group	Resource group 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 compartment-list

Parameter	Description	Type	Size	Default
compartment-id	OCI compartment ID.	string	Maximum length: 127	

config oci-region-list

Parameter	Description	Type	Size	Default
region	OCI region.	string	Maximum length: 31	

config external-ip

Parameter	Description	Type	Size	Default
name	External IP name.	string	Maximum length: 63	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	

config gcp-project-list

Parameter	Description	Type	Size	Default
id	GCP project ID.	string	Maximum length: 127	
gcp-zone-list <name>	Configure GCP zone list. GCP zone name.	string	Maximum length: 127	

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 system sdn-proxy

Configure SDN proxy.

```
config system sdn-proxy
  Description: Configure SDN proxy.
  edit <name>
    set type [general|fortimanager]
    set server {string}
    set server-port {integer}
    set username {string}
    set password {password_aes256}
  next
end
```

config system sdn-proxy

Parameter	Description	Type	Size	Default
name	SDN proxy name.	string	Maximum length: 35	
type	Type of SDN proxy.	option	-	general
	Option	Description		
	<i>general</i>	General HTTP proxy.		
	<i>fortimanager</i>	FortiManager SDN proxy.		
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

Parameter	Description	Type	Size	Default
username	SDN proxy username.	string	Maximum length: 64	
password	SDN proxy password.	password_aes256	Not Specified	

config system session

System IPv4 session.

```
config system session
    Description: System IPv4 session.
end
```

config system session6

System IPv6 session.

```
config system session6
    Description: System IPv6 session.
end
```

config system session-ttl

Configure global session TTL timers for this FortiProxy.

```
config system session-ttl
    Description: Configure global session TTL timers for this FortiProxy.
    set default {user}
    config port
        Description: Session TTL port.
        edit <id>
            set protocol {integer}
            set start-port {integer}
            set end-port {integer}
            set timeout {user}
            set refresh-direction [both|outgoing|...]
        next
    end
end
```

config system session-ttl

Parameter	Description	Type	Size	Default
default	Default timeout.	user	Not Specified	

config port

Parameter	Description	Type	Size	Default
id	Table entry ID.	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol (0 - 255).	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535	0
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535	0
timeout	Session timeout (TTL).	user	Not Specified	
refresh-direction	Configure refresh direction.	option	-	both
		Option	Description	
		<i>both</i>	Refresh both directions.	
		<i>outgoing</i>	Refresh outgoing direction (original).	
		<i>incoming</i>	Refresh incoming direction (reply).	

config system settings

Configure VDOM settings.

```
config system settings
  Description: Configure VDOM settings.
  set comments {var-string}
  set opmode [nat|transparent]
  set forward-domain [enable|disable]
  set http-external-dest [fortiweb|forticache]
  set firewall-session-dirty [check-all|check-new|...]
  set manageip {user}
  set gateway {ipv4-address}
  set ip {ipv4-classnet-host}
  set manageip6 {ipv6-prefix}
  set gateway6 {ipv6-address}
  set ip6 {ipv6-prefix}
  set device {string}
  set utf8-spam-tagging [enable|disable]
  set wccp-cache-engine [enable|disable]
  set wccp-local-route [enable|disable]
  set vpn-stats-log {option1}, {option2}, ...
  set vpn-stats-period {integer}
  set mac-ttl {integer}
  set fw-session-hairpin [enable|disable]
  set prp-trailer-action [enable|disable]
  set snat-hairpin-traffic [enable|disable]
  set dhcp-proxy [enable|disable]
  set dhcp-proxy-interface-select-method [auto|specify]
  set dhcp-proxy-interface {string}
  set dhcp-server-ip {user}
  set dhcp6-server-ip {user}
  set gui-default-policy-columns <name1>, <name2>, ...
  set link-down-access [enable|disable]
  set asymroute [enable|disable]
  set asymroute-icmp [enable|disable]
  set tcp-session-without-syn [enable|disable]
  set ses-denied-traffic [enable|disable]
  set strict-src-check [enable|disable]
  set allow-linkdown-path [enable|disable]
  set asymroute6 [enable|disable]
  set asymroute6-icmp [enable|disable]
  set sctp-session-without-init [enable|disable]
  set status [enable|disable]
  set allow-subnet-overlap [enable|disable]
  set deny-tcp-with-icmp [enable|disable]
  set discovered-device-timeout {integer}
  set email-portal-check-dns [disable|enable]
  set gui-proxy-inspection [enable|disable]
  set gui-icap [enable|disable]
  set gui-implicit-policy [enable|disable]
  set gui-dns-database [enable|disable]
  set gui-multicast-policy [enable|disable]
  set gui-dos-policy [enable|disable]
  set gui-object-colors [enable|disable]
  set gui-route-tag-address-creation [enable|disable]
```

```

set gui-voip-profile [enable|disable]
set gui-security-profile-group [enable|disable]
set gui-wanopt-cache [enable|disable]
set gui-explicit-proxy [enable|disable]
set gui-policy-based-ipsec [enable|disable]
set gui-threat-weight [enable|disable]
set gui-spamfilter [enable|disable]
set gui-file-filter [enable|disable]
set gui-application-control [enable|disable]
set gui-ips [enable|disable]
set gui-endpoint-control [enable|disable]
set gui-endpoint-control-advanced [enable|disable]
set gui-dhcp-advanced [enable|disable]
set gui-vpn [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-antivirus [enable|disable]
set gui-webfilter [enable|disable]
set gui-videofilter [enable|disable]
set gui-dnsfilter [enable|disable]
set gui-virtual-patch-profile [enable|disable]
set gui-dlp-profile [enable|disable]
set gui-advanced-policy [enable|disable]
set gui-allow-unnamed-policy [enable|disable]
set gui-email-collection [enable|disable]
set gui-multiple-interface-policy [enable|disable]
set gui-policy-disclaimer [enable|disable]
set gui-ztna [enable|disable]
set gui-ot [enable|disable]
set gui-dynamic-device-os-id [enable|disable]
set block-land-attack [disable|enable]
set default-app-port-as-service [enable|disable]
set application-bandwidth-tracking [disable|enable]
set default-policy-expiry-days {integer}
set gui-enforce-change-summary [disable|require|...]
set internet-service-database-cache [disable|enable]
end

```

config system settings

Parameter	Description	Type	Size	Default
comments	VDOM comments.	var-string	Maximum length: 255	
opmode	Firewall operation mode (NAT or Transparent).	option	-	nat

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>nat</i>	Change to NAT mode.		
	<i>transparent</i>	Change to transparent mode.		
forward-domain	Enable/disable forward domain.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable forward domain.		
	<i>disable</i>	Disable forward domain.		
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.		
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-	check-all
	Option	Description		
	<i>check-all</i>	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.		
	<i>check-new</i>	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.		
	<i>check-policy-option</i>	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.		
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified	
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default								
ip	IP address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified	::/0								
gateway6	Transparent mode IPv6 default gateway IP address.	ipv6-address	Not Specified	::								
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified	::/0								
device	Interface to use for management access for NAT mode.	string	Maximum length: 35									
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.											
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP cache engine.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP cache engine.</td></tr></table>				Option	Description	<i>enable</i>	Enable WCCP cache engine.	<i>disable</i>	Disable WCCP cache engine.		
Option	Description											
<i>enable</i>	Enable WCCP cache engine.											
<i>disable</i>	Disable WCCP cache engine.											
wccp-local-route	Enable/disable WCCP to use local route.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP to use local route.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP to use local route.</td></tr></table>				Option	Description	<i>enable</i>	Enable WCCP to use local route.	<i>disable</i>	Disable WCCP to use local route.		
Option	Description											
<i>enable</i>	Enable WCCP to use local route.											
<i>disable</i>	Disable WCCP to use local route.											
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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipsec</i></td><td>IPsec.</td></tr><tr><td><i>pptp</i></td><td>PPTP.</td></tr><tr><td><i>l2tp</i></td><td>L2TP.</td></tr></table>				Option	Description	<i>ipsec</i>	IPsec.	<i>pptp</i>	PPTP.	<i>l2tp</i>	L2TP.
Option	Description											
<i>ipsec</i>	IPsec.											
<i>pptp</i>	PPTP.											
<i>l2tp</i>	L2TP.											

Parameter	Description	Type	Size	Default						
vpn-stats-period	Period to send VPN log statistics (0 or 60 - 86400 sec).	integer	Minimum value: 0 Maximum value: 4294967295	600						
mac-ttl	Duration of MAC addresses in Transparent mode (300 - 8640000 sec, default = 300).	integer	Minimum value: 300 Maximum value: 8640000	300						
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiProxy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Perform a policy check every time.</td></tr><tr><td><i>disable</i></td><td>Perform a policy check only the first time the session is received.</td></tr></table>	Option	Description	<i>enable</i>	Perform a policy check every time.	<i>disable</i>	Perform a policy check only the first time the session is received.			
Option	Description									
<i>enable</i>	Perform a policy check every time.									
<i>disable</i>	Perform a policy check only the first time the session is received.									
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Try to keep PRP trailer.</td></tr><tr><td><i>disable</i></td><td>Trim PRP trailer.</td></tr></table>	Option	Description	<i>enable</i>	Try to keep PRP trailer.	<i>disable</i>	Trim PRP trailer.			
Option	Description									
<i>enable</i>	Try to keep PRP trailer.									
<i>disable</i>	Trim PRP trailer.									
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SNAT for hairpin traffic.</td></tr><tr><td><i>disable</i></td><td>Disable SNAT for hairpin traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable SNAT for hairpin traffic.	<i>disable</i>	Disable SNAT for hairpin traffic.			
Option	Description									
<i>enable</i>	Enable SNAT for hairpin traffic.									
<i>disable</i>	Disable SNAT for hairpin traffic.									
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-	disable						
	<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-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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified							
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified							
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79							
link-down-access	Enable/disable link down access traffic.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow link down access traffic.</td></tr><tr><td><i>disable</i></td><td>Block link down access traffic.</td></tr></table>	Option	Description	<i>enable</i>	Allow link down access traffic.	<i>disable</i>	Block link down access traffic.			
	Option	Description								
	<i>enable</i>	Allow link down access traffic.								
<i>disable</i>	Block link down access traffic.									
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPv4 asymmetric routing.</td></tr><tr><td><i>disable</i></td><td>Disable IPv4 asymmetric routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPv4 asymmetric routing.	<i>disable</i>	Disable IPv4 asymmetric routing.			
	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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICMP asymmetric routing.</td></tr><tr><td><i>disable</i></td><td>Disable ICMP asymmetric routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICMP asymmetric routing.	<i>disable</i>	Disable ICMP asymmetric routing.			
	Option	Description								
	<i>enable</i>	Enable ICMP asymmetric routing.								
<i>disable</i>	Disable ICMP asymmetric routing.									
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.									

Parameter	Description	Type	Size	Default						
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Include denied sessions in the session table.</td></tr><tr><td><i>disable</i></td><td>Do not add denied sessions to the session table.</td></tr></table>	Option	Description	<i>enable</i>	Include denied sessions in the session table.	<i>disable</i>	Do not add denied sessions to the session table.			
Option	Description									
<i>enable</i>	Include denied sessions in the session table.									
<i>disable</i>	Do not add denied sessions to the session table.									
strict-src-check	Enable/disable strict source verification.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict source verification.</td></tr><tr><td><i>disable</i></td><td>Disable strict source verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict source verification.	<i>disable</i>	Disable strict source verification.			
Option	Description									
<i>enable</i>	Enable strict source verification.									
<i>disable</i>	Disable strict source verification.									
allow-linkdown-path	Enable/disable link down path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow link down path.</td></tr><tr><td><i>disable</i></td><td>Do not allow link down path.</td></tr></table>	Option	Description	<i>enable</i>	Allow link down path.	<i>disable</i>	Do not allow link down path.			
Option	Description									
<i>enable</i>	Allow link down path.									
<i>disable</i>	Do not allow link down path.									
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable asymmetric IPv6 routing.</td></tr><tr><td><i>disable</i></td><td>Disable asymmetric IPv6 routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable asymmetric IPv6 routing.	<i>disable</i>	Disable asymmetric IPv6 routing.			
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable asymmetric ICMPv6 routing.</td></tr><tr><td><i>disable</i></td><td>Disable asymmetric ICMPv6 routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable asymmetric ICMPv6 routing.	<i>disable</i>	Disable asymmetric ICMPv6 routing.			
Option	Description									
<i>enable</i>	Enable asymmetric ICMPv6 routing.									
<i>disable</i>	Disable asymmetric ICMPv6 routing.									
sctp-session-without-init	Enable/disable SCTP session creation without SCTP INIT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SCTP session creation without SCTP INIT.</td></tr><tr><td><i>disable</i></td><td>Disable SCTP session creation without SCTP INIT.</td></tr></table>	Option	Description	<i>enable</i>	Enable SCTP session creation without SCTP INIT.	<i>disable</i>	Disable SCTP session creation without SCTP INIT.			
Option	Description									
<i>enable</i>	Enable SCTP session creation without SCTP INIT.									
<i>disable</i>	Disable SCTP session creation without SCTP INIT.									

Parameter	Description	Type	Size	Default
status	Enable/disable this VDOM.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this VDOM.		
	<i>disable</i>	Disable this VDOM.		
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.		
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-	disable
	Option	Description		
	<i>enable</i>	Deny TCP with ICMP.		
	<i>disable</i>	Disable denying TCP with ICMP.		
discovered-device-timeout	Timeout for discovered devices (1 - 365 days, default = 28).	integer	Minimum value: 1 Maximum value: 365	28
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable email address checking with DNS.		
	<i>enable</i>	Enable email address checking with DNS.		
gui-proxy-inspection	Enable/disable the proxy features on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the proxy features on the GUI.		
	<i>disable</i>	Disable the proxy features on the GUI.		
gui-icap	Enable/disable ICAP on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>enable</i>	Enable implicit firewall policies on the GUI.		
	<i>disable</i>	Disable implicit firewall policies 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-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable multicast firewall policies on the GUI.		
	<i>disable</i>	Disable multicast firewall policies on the GUI.		
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DoS policies on the GUI.		
	<i>disable</i>	Disable DoS policies on the GUI.		
gui-object-colors	Enable/disable object colors on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable object colors on the GUI.		
	<i>disable</i>	Disable object colors on the GUI.		
gui-route-tag-address-creation	Enable/disable route-tag addresses on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable route-tag addresses on the GUI.		
	<i>disable</i>	Disable route-tag addresses 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-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-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-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the explicit proxy on the GUI.		
	<i>disable</i>	Disable the explicit proxy on the GUI.		
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-	disable
	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-threat-weight	Enable/disable threat weight on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable threat weight on the GUI.		
	<i>disable</i>	Disable threat weight 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-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-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-ips	Enable/disable IPS on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS on the GUI.		
	<i>disable</i>	Disable IPS on the GUI.		
gui-endpoint-control	Enable/disable endpoint control on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable endpoint control on the GUI.		
	<i>disable</i>	Disable endpoint control on the GUI.		
gui-endpoint-control-advanced	Enable/disable advanced endpoint control options on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable advanced endpoint control options on the GUI.		
	<i>disable</i>	Disable advanced endpoint control options on the GUI.		
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-vpn	Enable/disable IPsec VPN settings pages on the GUI.	option	-	enable
	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-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-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-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-webfilter	Enable/disable Web filtering on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Web filtering on the GUI.		
	<i>disable</i>	Disable Web filtering 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-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.		
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-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-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable advanced policy configuration on the GUI.		
	<i>disable</i>	Disable advanced policy configuration on the GUI.		

Parameter	Description	Type	Size	Default						
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the requirement for policy naming on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable the requirement for policy naming on the GUI.</td></tr></table>	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.			
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-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-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-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-ztna	Enable/disable Zero Trust Network Access features on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Zero Trust Network Access features on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Zero Trust Network Access features on the GUI.</td></tr></table>	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.			
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.									
gui-ot	Enable/disable Operational technology features on the GUI.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Operational technology features on the GUI.		
	<i>disable</i>	Disable Operational technology features on the GUI.		
gui-dynamic-device-os-id	Enable/disable Create dynamic addresses to manage known devices.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Create dynamic addresses to manage known devices.		
	<i>disable</i>	Disable Create dynamic addresses to manage known devices.		
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.		
default-app-port-as-service	Enable/disable policy service enforcement based on application default ports.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
application-bandwidth-tracking	Enable/disable application bandwidth tracking.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable application bandwidth tracking.		
	<i>enable</i>	Enable application bandwidth tracking.		
default-policy-expiry-days	Default policy expiry in days (0 - 365 days, default = 30).	integer	Minimum value: 0 Maximum value: 365	30
gui-enforce-change-summary	Enforce change summaries for select tables in the GUI.	option	-	require

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	No change summary requirement.		
	<i>require</i>	Change summary required.		
	<i>optional</i>	Change summary optional.		
internet-service-database-cache	Enable/disable Internet Service database caching.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Internet Service database caching.		
	<i>enable</i>	Enable Internet Service database caching.		

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
name	Name of SMS server.	string	Maximum length: 35	
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	

config system snmp community

SNMP community configuration.

```

config system snmp community
    Description: SNMP community configuration.
    edit <id>
        set name {string}
        set status [enable|disable]
        config hosts
            Description: Configure IPv4 SNMP managers (hosts).
            edit <id>
                set source-ip {ipv4-address}
                set ip {user}
                set ha-direct [enable|disable]
                set host-type [any|query|...]
            next
        end
    config hosts6
        Description: Configure IPv6 SNMP managers.
        edit <id>
            set source-ipv6 {ipv6-address}
            set ipv6 {ipv6-prefix}
            set ha-direct [enable|disable]
            set host-type [any|query|...]
        next
    end
    set query-v1-status [enable|disable]
    set query-v1-port {integer}
    set query-v2c-status [enable|disable]
    set query-v2c-port {integer}
    set trap-v1-status [enable|disable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v2c-status [enable|disable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set events {option1}, {option2}, ...
    set mib-view {string}
    set vdoms <name1>, <name2>, ...
next
end

```

config system snmp community

Parameter	Description	Type	Size	Default
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Community name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
status	Enable/disable this SNMP community.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 1 Maximum value: 65535	161
query-v2c-status	Enable/disable SNMP v2c 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: 0 Maximum value: 65535	161
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trap-v1-lport	SNMP v1 trap local port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
trap-v1-rport	SNMP v1 trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	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

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 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 faz- disconnect faz load- balance-real- server-down per-cpu-high dhcp pool- usage cert-expiry
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.		

Parameter	Description	Type	Size	Default

Option	Description
<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 FortiProxy administrator and the FortiProxy is managed by FortiManager.
<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 FortiProxy enters conserve mode.
<i>av-bypass</i>	Send a trap when the FortiProxy enters bypass mode.
<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>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiProxy.

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>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>cert-expiry</i>	Send a trap when a local certificate is near expiry.		
mib-view	SNMP access control MIB view.	string	Maximum length: 32	
vdoms <name>	SNMP access control VDOMs. VDOM name.	string	Maximum length: 79	

config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified	0.0.0.0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	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
	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.		

config hosts6

Parameter	Description	Type	Size	Default
id	Host6 entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified	::
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified	::/0
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable
	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
	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.		

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 include {string}
    set exclude {string}
  next
end
```

config system snmp mib-view

Parameter	Description	Type	Size	Default
name	MIB view name.	string	Maximum length: 32	
include	OID subtrees to be included in the view. Maximum 16 allowed.	string	Maximum length: 79	
exclude	OID subtrees to be excluded in the view. Maximum 64 allowed.	string	Maximum length: 79	

config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
  Description: SNMP system info configuration.
  set status [enable|disable]
  set engine-id-type [text|hex|...]
  set engine-id {string}
  set description {var-string}
  set contact-info {var-string}
  set location {var-string}
  set trap-high-cpu-threshold {integer}
  set trap-low-memory-threshold {integer}
  set trap-log-full-threshold {integer}
  set trap-free-memory-threshold {integer}
  set trap-freeable-memory-threshold {integer}
  set append-index [enable|disable]
end
```

config system snmp sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
engine-id-type	Local SNMP engineID type (text/hex/mac).	option	-	text
	Option	Description		
	<i>text</i>	Text format.		
	<i>hex</i>	Octets format.		
	<i>mac</i>	MAC address format.		
engine-id	Local SNMP engineID string (maximum 27 characters).	string	Maximum length: 54	
description	System description.	var-string	Maximum length: 255	
contact-info	Contact information.	var-string	Maximum length: 255	
location	System location.	var-string	Maximum length: 255	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80
trap-low-memory-threshold	Memory 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-free-memory-threshold	Free memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	5

Parameter	Description	Type	Size	Default
trap-freeable-memory-threshold	Freeable memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	60
append-index	Enable/disable allowance of appending vdom or interface index in some RFC tables.	option	-	disable
	Option		Description	
	enable		Enable setting.	
	disable		Disable setting.	

config system snmp user

SNMP user configuration.

```

config system snmp user
  Description: SNMP user configuration.
  edit <name>
    set status [enable|disable]
    set trap-status [enable|disable]
    set trap-lport {integer}
    set trap-rport {integer}
    set queries [enable|disable]
    set query-port {integer}
    set notify-hosts {ipv4-address}
    set notify-hosts6 {ipv6-address}
    set source-ip {ipv4-address}
    set source-ipv6 {ipv6-address}
    set ha-direct [enable|disable]
    set events {option1}, {option2}, ...
    set mib-view {string}
    set vdoms <name1>, <name2>, ...
    set security-level [no-auth-no-priv|auth-no-priv|...]
    set auth-proto [md5|sha|...]
    set auth-pwd {password}
    set priv-proto [aes|des|...]
    set priv-pwd {password}
  next
end

```

config system snmp user

Parameter	Description	Type	Size	Default						
name	SNMP user name.	string	Maximum length: 32							
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-status	Enable/disable traps for 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						
trap-rport	SNMPv3 trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535	162						
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						
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified							

Parameter	Description	Type	Size	Default
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified	
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	::
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

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 ha-member- up ha- member- down ent- conf-change av-consume av-bypass av-oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open faz- disconnect faz load- balance-real- server-down per-cpu-high dhcp pool- usage cert- expiry
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.		

Parameter	Description	Type	Size	Default

Option	Description
<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 FortiProxy administrator and the FortiProxy is managed by FortiManager.
<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 FortiProxy enters conserve mode.
<i>av-bypass</i>	Send a trap when the FortiProxy enters bypass mode.
<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>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiProxy.

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>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>cert-expiry</i>	Send a trap when a local certificate is near expiry.		
mib-view	SNMP access control MIB view.	string	Maximum length: 32	
vdoms <name>	SNMP access control VDOMs. VDOM name.	string	Maximum length: 79	
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv
	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).		
auth-proto	Authentication protocol.	option	-	sha
	Option	Description		
	<i>md5</i>	HMAC-MD5-96 authentication protocol.		
	<i>sha</i>	HMAC-SHA-96 authentication protocol.		
	<i>sha224</i>	HMAC-SHA224 authentication protocol.		
	<i>sha256</i>	HMAC-SHA256 authentication protocol.		
	<i>sha384</i>	HMAC-SHA384 authentication protocol.		
	<i>sha512</i>	HMAC-SHA512 authentication protocol.		

Parameter	Description	Type	Size	Default										
auth-pwd	Password for authentication protocol.	password	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><tr><td><i>aes256cisco</i></td><td>CFB128-AES-256 symmetric encryption protocol compatible with CISCO.</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.	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.
	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.												
<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.													
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified											

config system source-ip status

Show configured service source-IP.

```
config system source-ip status
    Description: Show configured service source-IP.
end
```

config system span-port

Configure SPAN port.

```
config system span-port
    Description: Configure SPAN port.
    edit <id>
        set status [disable|enable]
        set span-source-port {string}
        set span-dest-port {string}
        set span-direction [rx|tx|...]
    next
end
```

config system span-port

Parameter	Description	Type	Size	Default
id	SPAN port id.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable SPAN.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable SPAN.	
		<i>enable</i>	Enable SPAN.	
span-source-port	SPAN source ports.	string	Maximum length: 15	
span-dest-port	SPAN destination port.	string	Maximum length: 15	
span-direction	SPAN direction.	option	-	both
		Option	Description	
		<i>rx</i>	Span receive direction only.	
		<i>tx</i>	Span transmit direction only.	
		<i>both</i>	Span both directions.	

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 status [disable|enable]
    set diffserv {user}
    set server-name {string}
    set mode [UDP|TCP|...]
    set schedules <name1>, <name2>, ...
    set dynamic-server [disable|enable]
    set ctrl-port {integer}
    set server-port {integer}
    set update-shaper [disable|local|...]
    set update-inbandwidth [disable|enable]
```

```

set update-outbandwidth [disable|enable]
set update-inbandwidth-maximum {integer}
set update-inbandwidth-minimum {integer}
set update-outbandwidth-maximum {integer}
set update-outbandwidth-minimum {integer}
next
end

```

config system speed-test-schedule

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
status	Enable/disable scheduled speed test.	option	-	enable
	Option Description			
	<i>disable</i>	Disable scheduled speed test.		
	<i>enable</i>	Enable scheduled speed test.		
diffserv	DSCP used for speed test.	user	Not Specified	
server-name	Speed test server name.	string	Maximum length: 35	
mode	Protocol Auto(default), TCP or UDP used for speed test.	option	-	Auto
	Option Description			
	<i>UDP</i>	Protocol UDP for speed test.		
	<i>TCP</i>	Protocol TCP for speed test.		
	<i>Auto</i>	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	
dynamic-server	Enable/disable dynamic server option.	option	-	disable
	Option Description			
	<i>disable</i>	Disable dynamic server.		
	<i>enable</i>	Enable dynamic server.The speed test server will be found automatically.		

Parameter	Description	Type	Size	Default
ctrl-port	Port of the controller to get access token.	integer	Minimum value: 1 Maximum value: 65535	5200
server-port	Port of the server to run speed test.	integer	Minimum value: 1 Maximum value: 65535	5201
update-shaper	Set egress shaper based on the test result.	option	-	disable
	Option Description			
	<i>disable</i>	Disable updating egress shaper.		
	<i>local</i>	Update local-side egress shaper.		
	<i>remote</i>	Update remote-side egress shaper.		
	<i>both</i>	Update both local-side and remote-side egress shaper.		
update-inbandwidth	Enable/disable bypassing interface's inbound bandwidth setting.	option	-	disable
	Option Description			
	<i>disable</i>	Honor interface's inbandwidth shaping.		
	<i>enable</i>	Ignore interface's inbandwidth shaping.		
update-outbandwidth	Enable/disable bypassing interface's outbound bandwidth setting.	option	-	disable
	Option Description			
	<i>disable</i>	Honor interface's outbandwidth shaping.		
	<i>enable</i>	Ignore updating interface's outbandwidth shaping.		
update-inbandwidth-maximum	Maximum downloading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0

Parameter	Description	Type	Size	Default
update-inbandwidth-minimum	Minimum downloading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0
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

config system speed-test-server

Configure speed test server list.

```

config system speed-test-server
    Description: Configure speed test server list.
    edit <name>
        set timestamp {integer}
        config host
            Description: Hosts of the server.
            edit <id>
                set ip {ipv4-address}
                set port {integer}
                set user {string}
                set password {password}
                set longitude {string}
                set latitude {string}
                set distance {integer}
            next
        end
    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	0

config host

Parameter	Description	Type	Size	Default
id	Server host ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Server host IPv4 address.	ipv4-address	Not Specified	0.0.0.0
port	Server host port number to communicate with client.	integer	Minimum value: 1 Maximum value: 65535	5204
user	Speed test host user name.	string	Maximum length: 64	
password	Speed test host password.	password	Not Specified	
longitude	Speed test host longitude.	string	Maximum length: 7	
latitude	Speed test host latitude.	string	Maximum length: 7	
distance	Speed test host distance.	integer	Minimum value: 0 Maximum value: 4294967295	0

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-kex-algo {option1}, {option2}, ...
  set ssh-enc-algo {option1}, {option2}, ...
  set ssh-mac-algo {option1}, {option2}, ...
  set ssh-hsk-algo {option1}, {option2}, ...
  set ssh-hsk-override [disable|enable]
  set ssh-hsk-password {password}
  set ssh-hsk {user}
end
```

config system ssh-config

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																								
<table><tr><th>Option</th><th>Description</th></tr><tr><td>diffie-hellman-group1-sha1</td><td>diffie-hellman-group1-sha1</td></tr><tr><td>diffie-hellman-group14-sha1</td><td>diffie-hellman-group14-sha1</td></tr><tr><td>diffie-hellman-group14-sha256</td><td>diffie-hellman-group14-sha256</td></tr><tr><td>diffie-hellman-group16-sha512</td><td>diffie-hellman-group16-sha512</td></tr><tr><td>diffie-hellman-group18-sha512</td><td>diffie-hellman-group18-sha512</td></tr><tr><td>diffie-hellman-group-exchange-sha1</td><td>diffie-hellman-group-exchange-sha1</td></tr><tr><td>diffie-hellman-group-exchange-sha256</td><td>diffie-hellman-group-exchange-sha256</td></tr><tr><td>curve25519-sha256@libssh.org</td><td>curve25519-sha256@libssh.org</td></tr><tr><td>ecdh-sha2-nistp256</td><td>ecdh-sha2-nistp256</td></tr><tr><td>ecdh-sha2-nistp384</td><td>ecdh-sha2-nistp384</td></tr><tr><td>ecdh-sha2-nistp521</td><td>ecdh-sha2-nistp521</td></tr></table>					Option	Description	diffie-hellman-group1-sha1	diffie-hellman-group1-sha1	diffie-hellman-group14-sha1	diffie-hellman-group14-sha1	diffie-hellman-group14-sha256	diffie-hellman-group14-sha256	diffie-hellman-group16-sha512	diffie-hellman-group16-sha512	diffie-hellman-group18-sha512	diffie-hellman-group18-sha512	diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha256	diffie-hellman-group-exchange-sha256	curve25519-sha256@libssh.org	curve25519-sha256@libssh.org	ecdh-sha2-nistp256	ecdh-sha2-nistp256	ecdh-sha2-nistp384	ecdh-sha2-nistp384	ecdh-sha2-nistp521	ecdh-sha2-nistp521
Option	Description																											
diffie-hellman-group1-sha1	diffie-hellman-group1-sha1																											
diffie-hellman-group14-sha1	diffie-hellman-group14-sha1																											
diffie-hellman-group14-sha256	diffie-hellman-group14-sha256																											
diffie-hellman-group16-sha512	diffie-hellman-group16-sha512																											
diffie-hellman-group18-sha512	diffie-hellman-group18-sha512																											
diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha1																											
diffie-hellman-group-exchange-sha256	diffie-hellman-group-exchange-sha256																											
curve25519-sha256@libssh.org	curve25519-sha256@libssh.org																											
ecdh-sha2-nistp256	ecdh-sha2-nistp256																											
ecdh-sha2-nistp384	ecdh-sha2-nistp384																											
ecdh-sha2-nistp521	ecdh-sha2-nistp521																											
ssh-enc-algo	Select one or more SSH ciphers.	option	-	aes256-ctr aes256-gcm@openssh.com																								

Parameter	Description	Type	Size	Default
	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		
	<i>aes128-gcm@openssh.com</i>	aes128-gcm@openssh.com		
<i>aes256-gcm@openssh.com</i>	aes256-gcm@openssh.com			
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		

Parameter	Description	Type	Size	Default																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hmac-md5-96-etm@openssh.com</i></td><td>hmac-md5-96-etm@openssh.com</td></tr><tr><td><i>hmac-sha1</i></td><td>hmac-sha1</td></tr><tr><td><i>hmac-sha1-etm@openssh.com</i></td><td>hmac-sha1-etm@openssh.com</td></tr><tr><td><i>hmac-sha2-256</i></td><td>hmac-sha2-256</td></tr><tr><td><i>hmac-sha2-256-etm@openssh.com</i></td><td>hmac-sha2-256-etm@openssh.com</td></tr><tr><td><i>hmac-sha2-512</i></td><td>hmac-sha2-512</td></tr><tr><td><i>hmac-sha2-512-etm@openssh.com</i></td><td>hmac-sha2-512-etm@openssh.com</td></tr><tr><td><i>hmac-ripemd160</i></td><td>hmac-ripemd160</td></tr><tr><td><i>hmac-ripemd160@openssh.com</i></td><td>hmac-ripemd160@openssh.com</td></tr><tr><td><i>hmac-ripemd160-etm@openssh.com</i></td><td>hmac-ripemd160-etm@openssh.com</td></tr><tr><td><i>umac-64@openssh.com</i></td><td>umac-64@openssh.com</td></tr><tr><td><i>umac-128@openssh.com</i></td><td>umac-128@openssh.com</td></tr><tr><td><i>umac-64-etm@openssh.com</i></td><td>umac-64-etm@openssh.com</td></tr><tr><td><i>umac-128-etm@openssh.com</i></td><td>umac-128-etm@openssh.com</td></tr></table>		Option	Description	<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			
	Option	Description																																	
	<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																																		
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																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssh-rsa</i></td><td>ssh-rsa</td></tr><tr><td><i>ecdsa-sha2-nistp521</i></td><td>ecdsa-sha2-nistp521</td></tr></table>		Option	Description	<i>ssh-rsa</i>	ssh-rsa	<i>ecdsa-sha2-nistp521</i>	ecdsa-sha2-nistp521																											
	Option	Description																																	
	<i>ssh-rsa</i>	ssh-rsa																																	
<i>ecdsa-sha2-nistp521</i>	ecdsa-sha2-nistp521																																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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	
ssh-hsk	Config SSH host key.	user	Not Specified	

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
name	SSO admin name.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
accprofile	SSO admin user access profile.	string	Maximum length: 35	
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
name	FortiCloud SSO admin name.	string	Maximum length: 64	
accprofile	FortiCloud SSO admin user access profile.	string	Maximum length: 35	
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
name	FortiCloud SSO admin name.	string	Maximum length: 64	
accprofile	FortiCloud SSO admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system startup-error-log

Display startup config error on console.

```
config system startup-error-log
    Description: Display startup config error on console.
end
```

config system status

System status.

```
config system status
    Description: System status.
end
```

config system storage

Configure logical storage.

```
config system storage
    Description: Configure logical storage.
    edit <name>
        set status [enable|disable]
        set media-status [enable|disable|...]
        set order {integer}
        set partition {string}
        set device {string}
        set size {integer}
        set usage [log|wanopt]
        set wanopt-mode [mix|wanopt|...]
```



```
next
end
```

config system storage

Parameter	Description	Type	Size	Default
name	Storage name.	string	Maximum length: 35	default_n
status	Enable/disable storage.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
media-status	The physical status of current media.	option	-	disable
	Option	Description		
	enable	Storage is enabled.		
	disable	Storage is disabled.		
	fail	Storage have some fail sector.		
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255	0
partition	Label of underlying partition.	string	Maximum length: 16	<unknown>
device	Partition device.	string	Maximum length: 19	?
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.		

Parameter	Description	Type	Size	Default
wanopt-mode	WAN Optimization mode (default=webcache)	option	-	webcache
	Option	Description		
	<i>mix</i>	Use hard disk for WAN Optimization mix mode.		
	<i>wanopt</i>	Use hard disk for WAN Optimization wanopt mode.		
	<i>webcache</i>	Use hard disk for WAN Optimization webcache mode.		

config system timezone

Show timezone.

```
config system timezone
  Description: Show timezone.
  edit <name>
  next
end
```

config system timezone

Parameter	Description	Type	Size	Default
name	Database name of a timezone.	string	Maximum length: 63	

config system vdom

Configure virtual domain.

```
config system vdom
  Description: Configure virtual domain.
  edit <name>
    set short-name {string}
    set vcluster-id {integer}
    set flag {integer}
  next
end
```

config system vdom

Parameter	Description	Type	Size	Default
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
flag	Flag.	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 vdom-dns [enable|disable]
  set primary {ipv4-address}
  set secondary {ipv4-address}
  set protocol {option1}, {option2}, ...
  set ssl-certificate {string}
  set server-hostname <hostname1>, <hostname2>, ...
  set ip6-primary {ipv6-address}
  set ip6-secondary {ipv6-address}
  set source-ip {ipv4-address}
  set interface-select-method [auto|specify]
  set interface {string}
  set server-select-method [least-rtt|failover]
  set alt-primary {ipv4-address}
  set alt-secondary {ipv4-address}
end
```

config system vdom-dns

Parameter	Description	Type	Size	Default
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-	disable
	Option Description			
	enable	Enable configuring DNS servers for the current VDOM.		
	disable	Disable configuring DNS servers for the current VDOM.		
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0
protocol	DNS transport protocols.	option	-	cleartext
	Option Description			
	cleartext	DNS over UDP/53, DNS over TCP/53.		
	dot	DNS over TLS/853.		
	doh	DNS over HTTPS/443.		
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127	
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	::
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option Description			
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		

Parameter	Description	Type	Size	Default						
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
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.									
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						

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	-	

Parameter	Description	Type	Size	Default
	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		
	<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.snmp.sysinfo</i>	system.snmp.sysinfo		
	<i>system.snmp.community</i>	system.snmp.community		
	<i>system.snmp.user</i>	system.snmp.user		
	<i>system.interface</i>	system.interface		
	<i>vpn.ipsec.phase1-interface</i>	vpn.ipsec.phase1-interface		

Parameter	Description	Type	Size	Default																																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vpn.ipsec.phase2-interface</i></td><td>vpn.ipsec.phase2-interface</td></tr><tr><td><i>router.bgp</i></td><td>router.bgp</td></tr><tr><td><i>router.route-map</i></td><td>router.route-map</td></tr><tr><td><i>router.prefix-list</i></td><td>router.prefix-list</td></tr><tr><td><i>firewall.ippool</i></td><td>firewall.ippool</td></tr><tr><td><i>firewall.ippool6</i></td><td>firewall.ippool6</td></tr><tr><td><i>router.static</i></td><td>router.static</td></tr><tr><td><i>router.static6</i></td><td>router.static6</td></tr><tr><td><i>firewall.vip</i></td><td>firewall.vip</td></tr><tr><td><i>firewall.vip6</i></td><td>firewall.vip6</td></tr><tr><td><i>system.sdwan</i></td><td>system.sdwan</td></tr><tr><td><i>system.saml</i></td><td>system.saml</td></tr><tr><td><i>router.policy</i></td><td>router.policy</td></tr><tr><td><i>router.policy6</i></td><td>router.policy6</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>vpn.ipsec.phase2-interface</i>	vpn.ipsec.phase2-interface	<i>router.bgp</i>	router.bgp	<i>router.route-map</i>	router.route-map	<i>router.prefix-list</i>	router.prefix-list	<i>firewall.ippool</i>	firewall.ippool	<i>firewall.ippool6</i>	firewall.ippool6	<i>router.static</i>	router.static	<i>router.static6</i>	router.static6	<i>firewall.vip</i>	firewall.vip	<i>firewall.vip6</i>	firewall.vip6	<i>system.sdwan</i>	system.sdwan	<i>system.saml</i>	system.saml	<i>router.policy</i>	router.policy	<i>router.policy6</i>	router.policy6	<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>vpn.ipsec.phase2-interface</i>	vpn.ipsec.phase2-interface																																							
	<i>router.bgp</i>	router.bgp																																							
	<i>router.route-map</i>	router.route-map																																							
	<i>router.prefix-list</i>	router.prefix-list																																							
	<i>firewall.ippool</i>	firewall.ippool																																							
	<i>firewall.ippool6</i>	firewall.ippool6																																							
	<i>router.static</i>	router.static																																							
	<i>router.static6</i>	router.static6																																							
	<i>firewall.vip</i>	firewall.vip																																							
	<i>firewall.vip6</i>	firewall.vip6																																							
	<i>system.sdwan</i>	system.sdwan																																							
	<i>system.saml</i>	system.saml																																							
	<i>router.policy</i>	router.policy																																							
	<i>router.policy6</i>	router.policy6																																							
	<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>
    next
  end
```

config system vdom-link

Parameter	Description	Type	Size	Default
name	VDOM link name (maximum = 11 characters).	string	Maximum length: 11	

config system vdom-property

Configure VDOM property.

```
config system vdom-property
  Description: Configure VDOM property.
  edit <name>
    set description {string}
    set snmp-index {integer}
    set ipsec-phase1-interface {user}
    set ipsec-phase2-interface {user}
    set firewall-policy {user}
    set firewall-address {user}
    set firewall-addrgroup {user}
    set custom-service {user}
    set service-group {user}
    set onetime-schedule {user}
    set recurring-schedule {user}
    set user {user}
    set user-group {user}
    set proxy {user}
    set log-disk-quota {user}
  next
end
```


config system vdom-property

Parameter	Description	Type	Size	Default
name	VDOM name.	string	Maximum length: 31	
description	Description.	string	Maximum length: 127	
snmp-index	Permanent SNMP Index of the virtual domain (1 - 2147483647).	integer	Minimum value: 1 Maximum value: 2147483647	0
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified	
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified	
firewall-policy	Maximum guaranteed number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	user	Not Specified	
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified	
firewall-addrgroup	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified	
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified	
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified	
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified	
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified	
user	Maximum guaranteed number of local users.	user	Not Specified	
user-group	Maximum guaranteed number of user groups.	user	Not Specified	
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified	

Parameter	Description	Type	Size	Default
log-disk-quota	Log disk quota in megabytes (MB). Range depends on how much disk space is available.	user	Not Specified	

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 status [enable|disable]
        set radius-server-vdom {string}
    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	
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.		
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	

config system vne-tunnel

Configure virtual network enabler tunnel.

```
config system vne-tunnel
    Description: Configure virtual network enabler tunnel.
    set status [enable|disable]
    set interface {string}
```

```

set ssl-certificate {string}
set bmr-hostname {password}
set ipv4-address {ipv4-classnet-host}
set br {string}
set update-url {string}
set mode [map-e|fixed-ip|...]
set http-username {string}
set http-password {password}
end

```

config system vne-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable VNE tunnel.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable VNE tunnel.		
	<i>disable</i>	Disable VNE tunnel.		
interface	Interface name.	string	Maximum length: 15	
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
bmr-hostname	BMR hostname.	password	Not Specified	
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
br	IPv6 address or FQDN of the border relay.	string	Maximum length: 255	
update-url	URL of provisioning server.	string	Maximum length: 511	
mode	VNE tunnel mode.	option	-	map-e
	Option	Description		
	<i>map-e</i>	Map-e mode.		
	<i>fixed-ip</i>	Fixed-ip mode.		
	<i>ds-lite</i>	DS-Lite mode.		
http-username	HTTP authentication user name.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
http-password	HTTP authentication password.	password	Not Specified	

config system vxlan

Configure VXLAN devices.

```

config system vxlan
    Description: Configure VXLAN devices.
    edit <name>
        set interface {string}
        set vni {integer}
        set ip-version [ipv4-unicast|ipv6-unicast]
        set remote-ip <ip1>, <ip2>, ...
        set remote-ip6 <ip61>, <ip62>, ...
        set dstport {integer}
        set multicast-ttl {integer}
        set evpn-id {integer}
        set learn-from-traffic [enable|disable]
    next
end

```

config system vxlan

Parameter	Description	Type	Size	Default						
name	VXLAN device or interface name. Must be a unique interface name.	string	Maximum length: 15							
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15							
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215	0						
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. 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 VXLAN.</td></tr><tr><td>ipv6-unicast</td><td>Use IPv6 unicast 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.
Option	Description									
ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.									
ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.									

Parameter	Description	Type	Size	Default
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	
dstport	VXLAN destination port (1 - 65535, default = 4789).	integer	Minimum value: 1 Maximum value: 65535	4789
multicast-ttl	VXLAN multicast TTL (1-255, default = 0).	integer	Minimum value: 1 Maximum value: 255	0
evpn-id	EVPN instance.	integer	Minimum value: 1 Maximum value: 65535	0
learn-from-traffic	Enable/disable VXLAN MAC learning from traffic.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable VXLAN MAC learning from traffic.	
		<i>disable</i>	Disable VXLAN MAC learning from traffic.	

config system wccp

Configure WCCP.

```
config system wccp
  Description: Configure WCCP.
  edit <service-id>
    set router-id {ipv4-address}
    set cache-id {ipv4-address}
    set group-address {ipv4-address-multicast}
    set server-list {user}
    set router-list {user}
    set ports-defined [source|destination]
    set server-type [forward|proxy]
    set ports {user}
```

```

set authentication [enable|disable]
set password {password}
set forward-method [GRE|L2|...]
set cache-engine-method [GRE|L2]
set service-type [auto|standard|...]
set primary-hash {option1}, {option2}, ...
set priority {integer}
set protocol {integer}
set assignment-weight {integer}
set assignment-bucket-format [wccp-v2|cisco-implementation]
set return-method [GRE|L2|...]
set assignment-method [HASH|MASK|...]
set assignment-srcaddr-mask {ipv4-netmask-any}
set assignment-dstaddr-mask {ipv4-netmask-any}
next
end

```

config system wccp

Parameter	Description	Type	Size	Default						
service-id	Service ID.	string	Maximum length: 3							
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiProxy interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0						
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						
group-address	IP multicast address used by the cache routers. For the FortiProxy to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified	0.0.0.0						
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified							
router-list	IP addresses of one or more WCCP routers.	user	Not Specified							
ports-defined	Match method.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>source</td><td>Source port match.</td></tr><tr><td>destination</td><td>Destination port match.</td></tr></table>				Option	Description	source	Source port match.	destination	Destination port match.
Option	Description									
source	Source port match.									
destination	Destination port match.									

Parameter	Description	Type	Size	Default								
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.											
ports	Service ports.	user	Not Specified									
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.											
password	Password for MD5 authentication.	password	Not Specified									
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.											
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.											
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></table>	Option	Description	<i>auto</i>	auto							
Option	Description											
<i>auto</i>	auto											

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></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>standard</i>	Standard service.	<i>dynamic</i>	Dynamic service.							
	Option	Description												
	<i>standard</i>	Standard service.												
<i>dynamic</i>	Dynamic service.													
primary-hash	Hash method.	option	-	dst-ip										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>src-ip</i></td><td>Source IP hash.</td></tr><tr><td><i>dst-ip</i></td><td>Destination IP hash.</td></tr><tr><td><i>src-port</i></td><td>Source port hash.</td></tr><tr><td><i>dst-port</i></td><td>Destination port hash.</td></tr></table>	Option	Description	<i>src-ip</i>	Source IP hash.	<i>dst-ip</i>	Destination IP hash.	<i>src-port</i>	Source port hash.	<i>dst-port</i>	Destination port hash.			
	Option	Description												
	<i>src-ip</i>	Source IP hash.												
	<i>dst-ip</i>	Destination IP hash.												
	<i>src-port</i>	Source port hash.												
<i>dst-port</i>	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										
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255	0										
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-	cisco-implementation										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wccp-v2</i></td><td>WCCP-v2 bucket format.</td></tr><tr><td><i>cisco-implementation</i></td><td>Cisco bucket format.</td></tr></table>	Option	Description	<i>wccp-v2</i>	WCCP-v2 bucket format.	<i>cisco-implementation</i>	Cisco bucket format.							
	Option	Description												
	<i>wccp-v2</i>	WCCP-v2 bucket format.												
<i>cisco-implementation</i>	Cisco bucket format.													
return-method	Method used to decline a redirected packet and return it to the FortiProxy unit.	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.													

Parameter	Description	Type	Size	Default
assignment-method	Hash key assignment preference.	option	-	HASH
	Option	Description		
	<i>HASH</i>	HASH assignment method.		
	<i>MASK</i>	MASK assignment method.		
	<i>any</i>	HASH or MASK.		
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified	0.0.23.65
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified	0.0.0.0

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>
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
        set description {string}
        set interface <interface-name1>, <interface-name2>, ...
    next
end

```

config system zone

Parameter	Description	Type	Size	Default
name	Zone name.	string	Maximum length: 35	

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	

config tagging

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

test

This section includes syntax for the following commands:

- [config test acd on page 1153](#)
- [config test acsd on page 1153](#)
- [config test autod on page 1153](#)
- [config test awsd on page 1154](#)
- [config test azd on page 1154](#)
- [config test bfd on page 1154](#)
- [config test cloudapid on page 1155](#)
- [config test cmdbsvr on page 1155](#)
- [config test csfd on page 1156](#)
- [config test ddnsd on page 1156](#)
- [config test dhcp6c on page 1156](#)
- [config test dhcp6r on page 1157](#)
- [config test dhcprelay on page 1157](#)
- [config test dlpfingerprint on page 1157](#)
- [config test dlpfpcache on page 1158](#)
- [config test dnsproxy on page 1158](#)
- [config test dsd on page 1159](#)
- [config test eap_supp on page 1159](#)
- [config test evpn on page 1159](#)
- [config test fas on page 1160](#)
- [config test fcnacd on page 1160](#)
- [config test fds_notify on page 1160](#)
- [config test fgtlogd on page 1161](#)
- [config test fnbamd on page 1161](#)
- [config test forticldd on page 1162](#)
- [config test forticron on page 1162](#)
- [config test fsd on page 1162](#)
- [config test fsvrd on page 1163](#)
- [config test gcpcd on page 1163](#)
- [config test harelay on page 1163](#)
- [config test hasync on page 1164](#)
- [config test hataalk on page 1164](#)
- [config test ibmd on page 1165](#)
- [config test imap on page 1165](#)
- [config test init on page 1165](#)
- [config test iotd on page 1166](#)

-
- [config test ipamd on page 1166](#)
 - [config test ipamsd on page 1166](#)
 - [config test ipldbd on page 1167](#)
 - [config test ipsengine on page 1167](#)
 - [config test ipsmonitor on page 1168](#)
 - [config test ipsufd on page 1168](#)
 - [config test kmipd on page 1168](#)
 - [config test kubed on page 1169](#)
 - [config test l2tpcd on page 1169](#)
 - [config test lnkmttd on page 1169](#)
 - [config test locallogd on page 1170](#)
 - [config test miglogd on page 1170](#)
 - [config test mrd on page 1171](#)
 - [config test netxd on page 1171](#)
 - [config test nntp on page 1171](#)
 - [config test ocid on page 1172](#)
 - [config test openstackd on page 1172](#)
 - [config test ovrd on page 1172](#)
 - [config test pcpcd on page 1173](#)
 - [config test pop3 on page 1173](#)
 - [config test pptpcd on page 1174](#)
 - [config test quarantined on page 1174](#)
 - [config test radius-das on page 1175](#)
 - [config test radiusd on page 1174](#)
 - [config test radvd on page 1175](#)
 - [config test reportd on page 1175](#)
 - [config test sdncd on page 1176](#)
 - [config test sdnd on page 1176](#)
 - [config test sepmd on page 1177](#)
 - [config test sessionsync on page 1177](#)
 - [config test sfupgraded on page 1177](#)
 - [config test smtp on page 1178](#)
 - [config test snmpd on page 1178](#)
 - [config test syslogd on page 1178](#)
 - [config test updated on page 1179](#)
 - [config test uploadd on page 1179](#)
 - [config test urlfilter on page 1180](#)
 - [config test vned on page 1180](#)
 - [config test wad on page 1180](#)
 - [config test wccpd on page 1181](#)
 - [config test wf_monitor on page 1181](#)
 - [config test wiredapd on page 1181](#)

config test acd

Aggregate Controller.

```
config test acd
  Description: Aggregate Controller.
  set <Integer> {string}
end
```

config test acd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test acsd

Ali Cloud Service daemon.

```
config test acsd
  Description: Ali Cloud Service daemon.
  set <Integer> {string}
end
```

config test acsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test autod

Automation daemon.

```
config test autod
  Description: Automation daemon.
  set <Integer> {string}
end
```

config test autod

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test awsd

Amazon Web Services (AWS) daemon.

```
config test awsd
  Description: Amazon Web Services (AWS) daemon.
  set <Integer> {string}
end
```

config test awsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test azd

Microsoft Azure daemon.

```
config test azd
  Description: Microsoft Azure daemon.
  set <Integer> {string}
end
```

config test azd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test bfd

BFD daemon.

```
config test bfd
  Description: BFD daemon.
  set <Integer> {string}
end
```

config test bfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test clouapid

Cloud service communication daemon.

```
config test clouapid
  Description: Cloud service communication daemon.
  set <Integer> {string}
end
```

config test clouapid

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test cmdbsvr

cmdb server

```
config test cmdbsvr
  Description: cmdb server
  set <Integer> {string}
end
```

config test cmdbsvr

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test csfd

Security Fabric daemon.

```
config test csfd
  Description: Security Fabric daemon.
  set <Integer> {string}
end
```

config test csfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ddnsd

DDNS client daemon.

```
config test ddnsd
  Description: DDNS client daemon.
  set <Integer> {string}
end
```

config test ddnsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dhcp6c

DHCP6 client daemon.

```
config test dhcp6c
  Description: DHCP6 client daemon.
  set <Integer> {string}
end
```


config test dhcp6c

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dhcp6r

DHCP6 relay daemon.

```
config test dhcp6r
  Description: DHCP6 relay daemon.
  set <Integer> {string}
end
```

config test dhcp6r

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dhcprelay

DHCP relay daemon.

```
config test dhcprelay
  Description: DHCP relay daemon.
  set <Integer> {string}
end
```

config test dhcprelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dlpfingerprint

DLP fingerprint daemon.

```
config test dlpfingerprint
  Description: DLP fingerprint daemon.
  set <Integer> {string}
end
```

config test dlpfingerprint

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dlpfpcache

DLP fingerprint cache daemon.

```
config test dlpfpcache
  Description: DLP fingerprint cache daemon.
  set <Integer> {string}
end
```

config test dlpfpcache

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dnsproxy

DNS proxy.

```
config test dnsproxy
  Description: DNS proxy.
  set <Integer> {string}
end
```

config test dnsproxy

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dsd

DLP Statistics daemon.

```
config test dsd
  Description: DLP Statistics daemon.
  set <Integer> {string}
end
```

config test dsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test eap_supp

EAP Supplicant daemon.

```
config test eap_supp
  Description: EAP Supplicant daemon.
  set <Integer> {string}
end
```

config test eap_supp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test evpn

EVPN daemon.

```
config test evpn
  Description: EVPN daemon.
  set <Integer> {string}
end
```

config test evpn

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fas

FortiToken Cloud daemon.

```
config test fas
  Description: FortiToken Cloud daemon.
  set <Integer> {string}
end
```

config test fas

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fcnacd

FortiClient NAC daemon.

```
config test fcnacd
  Description: FortiClient NAC daemon.
  set <Integer> {string}
end
```

config test fcnacd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fds_notify

Update Notification daemon.

```
config test fds_notify
  Description: Update Notification daemon.
  set <Integer> {string}
end
```

config test fds_notify

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fgtlogd

Fgtlog daemon.

```
config test fgtlogd
  Description: Fgtlog daemon.
  set <Integer> {string}
end
```

config test fgtlogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fnbamd

FortiGate non-blocking auth daemon.

```
config test fnbamd
  Description: FortiGate non-blocking auth daemon.
  set <Integer> {string}
end
```

config test fnbamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test forticldd

FortiCloud daemon.

```
config test forticldd
  Description: FortiCloud daemon.
  set <Integer> {string}
end
```

config test forticldd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test forticron

Forticron daemon.

```
config test forticron
  Description: Forticron daemon.
  set <Integer> {string}
end
```

config test forticron

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fsd

FortiExplorer daemon.

```
config test fsd
  Description: FortiExplorer daemon.
  set <Integer> {string}
end
```

config test fsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fsvrd

FortiService daemon.

```
config test fsvrd
  Description: FortiService daemon.
  set <Integer> {string}
end
```

config test fsvrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test gcpd

Google Cloud Platform (GCP) daemon.

```
config test gcpd
  Description: Google Cloud Platform (GCP) daemon.
  set <Integer> {string}
end
```

config test gcpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test harelay

HA relay daemon.

```
config test harelay
  Description: HA relay daemon.
  set <Integer> {string}
end
```

config test harelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test hasync

HA sync daemon.

```
config test hasync
  Description: HA sync daemon.
  set <Integer> {string}
end
```

config test hasync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test hataalk

HA talk daemon.

```
config test hataalk
  Description: HA talk daemon.
  set <Integer> {string}
end
```

config test hataalk

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ibmd

IBM Cloud Infrastructure daemon.

```
config test ibmd
  Description: IBM Cloud Infrastructure daemon.
  set <Integer> {string}
end
```

config test ibmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test imap

IMAP proxy.

```
config test imap
  Description: IMAP proxy.
  set <Integer> {string}
end
```

config test imap

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test init

init process.

```
config test init
  Description: init process.
  set <Integer> {string}
end
```

config test init

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test iotd

IoT device info daemon.

```
config test iotd
  Description: IoT device info daemon.
  set <Integer> {string}
end
```

config test iotd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipamd

IP Address Management daemon.

```
config test ipamd
  Description: IP Address Management daemon.
  set <Integer> {string}
end
```

config test ipamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipamsd

IPAM server daemon.

```
config test ipamsd
  Description: IPAM server daemon.
  set <Integer> {string}
end
```

config test ipamsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipdbd

IP load balancing daemon.

```
config test ipdbd
  Description: IP load balancing daemon.
  set <Integer> {string}
end
```

config test ipdbd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipsengine

IPS sensor.

```
config test ipsengine
  Description: IPS sensor.
  set <Integer> {string}
end
```

config test ipsengine

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipsmonitor

IPS monitor.

```
config test ipsmonitor
  Description: IPS monitor.
  set <Integer> {string}
end
```

config test ipsmonitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipsufd

IPS urlfilter daemon.

```
config test ipsufd
  Description: IPS urlfilter daemon.
  set <Integer> {string}
end
```

config test ipsufd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test kmipd

KMIP daemon.

```
config test kmipd
  Description: KMIP daemon.
  set <Integer> {string}
end
```

config test kmipd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test kubed

Kubernetes daemon.

```
config test kubed
  Description: Kubernetes daemon.
  set <Integer> {string}
end
```

config test kubed

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test l2tpcd

L2TP client daemon.

```
config test l2tpcd
  Description: L2TP client daemon.
  set <Integer> {string}
end
```

config test l2tpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test lnkmttd

Link monitor daemon.

```
config test lnkmtd
  Description: Link monitor daemon.
  set <Integer> {string}
end
```

config test lnkmtd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test locallogd

Locallogd daemon.

```
config test locallogd
  Description: Locallogd daemon.
  set <Integer> {string}
end
```

config test locallogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test miglogd

Miglog logging daemon.

```
config test miglogd
  Description: Miglog logging daemon.
  set <Integer> {string}
end
```

config test miglogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test mrd

Mobile router daemon.

```
config test mrd
    Description: Mobile router daemon.
    set <Integer> {string}
end
```

config test mrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test netxd

VMWare NetX service manager daemon.

```
config test netxd
    Description: VMWare NetX service manager daemon.
    set <Integer> {string}
end
```

config test netxd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test nntp

NNTP proxy.

```
config test nntp
    Description: NNTP proxy.
    set <Integer> {string}
end
```

config test nntp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ocid

Oracle Cloud Infrastructure.

```
config test ocid
  Description: Oracle Cloud Infrastructure.
  set <Integer> {string}
end
```

config test ocid

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test openstackd

OpenStack SDN connector daemon.

```
config test openstackd
  Description: OpenStack SDN connector daemon.
  set <Integer> {string}
end
```

config test openstackd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ovrd

Override daemon.


```
config test ovrld
  Description: Override daemon.
  set <Integer> {string}
end
```

config test ovrld

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test pcpd

PCP server daemon.

```
config test pcpd
  Description: PCP server daemon.
  set <Integer> {string}
end
```

config test pcpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test pop3

POP3 proxy.

```
config test pop3
  Description: POP3 proxy.
  set <Integer> {string}
end
```

config test pop3

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test pptpcd

PPTP client.

```
config test pptpcd
  Description: PPTP client.
  set <Integer> {string}
end
```

config test pptpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test quarantined

Quarantine daemon.

```
config test quarantined
  Description: Quarantine daemon.
  set <Integer> {string}
end
```

config test quarantined

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test radiusd

RADIUS daemon.

```
config test radiusd
  Description: RADIUS daemon.
  set <Integer> {string}
end
```

config test radiusd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test radius-das

Radius-das daemon.

```
config test radius-das
  Description: Radius-das daemon.
  set <Integer> {string}
end
```

config test radius-das

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test radvd

radvd daemon.

```
config test radvd
  Description: radvd daemon.
  set <Integer> {string}
end
```

config test radvd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test reportd

Report daemon.

```
config test reportd
  Description: Report daemon.
  set <Integer> {string}
end
```

config test reportd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sdncd

SDN Connector daemon.

```
config test sdncd
  Description: SDN Connector daemon.
  set <Integer> {string}
end
```

config test sdncd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sdnd

SDN connector daemon.

```
config test sdnd
  Description: SDN connector daemon.
  set <Integer> {string}
end
```

config test sdnd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sepmd

Symantec Endpoint Protection Manager daemon.

```
config test sepmd
  Description: Symantec Endpoint Protection Manager daemon.
  set <Integer> {string}
end
```

config test sepmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sessionsync

Session sync daemon.

```
config test sessionsync
  Description: Session sync daemon.
  set <Integer> {string}
end
```

config test sessionsync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sfupgraded

Security Fabric Upgrade daemon.

```
config test sfupgraded
  Description: Security Fabric Upgrade daemon.
  set <Integer> {string}
end
```

config test sfupgraded

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test smtp

SMTP proxy.

```
config test smtp
  Description: SMTP proxy.
  set <Integer> {string}
end
```

config test smtp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test snmpd

SNMP daemon.

```
config test snmpd
  Description: SNMP daemon.
  set <Integer> {string}
end
```

config test snmpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test syslogd

Syslog daemon.

```
config test syslogd
  Description: Syslog daemon.
  set <Integer> {string}
end
```

config test syslogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test updated

Update daemon.

```
config test updated
  Description: Update daemon.
  set <Integer> {string}
end
```

config test updated

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test uploadd

Upload daemon.

```
config test uploadd
  Description: Upload daemon.
  set <Integer> {string}
end
```

config test uploadd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test urlfilter

URL filter daemon.

```
config test urlfilter
  Description: URL filter daemon.
  set <Integer> {string}
end
```

config test urlfilter

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test vned

Virtual network enabler daemon.

```
config test vned
  Description: Virtual network enabler daemon.
  set <Integer> {string}
end
```

config test vned

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wad

WAD related processes.

```
config test wad
  Description: WAD related processes.
  set <Integer> {string}
end
```

config test wad

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wccpd

WCCP daemon.

```
config test wccpd
  Description: WCCP daemon.
  set <Integer> {string}
end
```

config test wccpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wf_monitor

WF monitor.

```
config test wf_monitor
  Description: WF monitor.
  set <Integer> {string}
end
```

config test wf_monitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wiredapd

Wiredapd daemon.

```
config test wiredapd
  Description: Wiredapd daemon.
  set <Integer> {string}
end
```

config test wiredapd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

user

This section includes syntax for the following commands:

- [config user adgrp on page 1183](#)
- [config user certificate on page 1184](#)
- [config user domain-controller on page 1185](#)
- [config user exchange on page 1189](#)
- [config user external-identity-provider on page 1192](#)
- [config user fortitoken on page 1194](#)
- [config user fsso-polling on page 1199](#)
- [config user fsso on page 1195](#)
- [config user group on page 1201](#)
- [config user krb-keytab on page 1206](#)
- [config user ldap on page 1207](#)
- [config user local on page 1216](#)
- [config user oidc on page 1220](#)
- [config user password-policy on page 1223](#)
- [config user peer on page 1225](#)
- [config user peergrp on page 1227](#)
- [config user pop3 on page 1227](#)
- [config user radius on page 1229](#)
- [config user saml on page 1244](#)
- [config user security-exempt-list on page 1248](#)
- [config user setting on page 1249](#)
- [config user tacacs+ on page 1254](#)

config user adgrp

Configure FSSO groups.

```
config user adgrp
  Description: Configure FSSO groups.
  edit <name>
    set server-name {string}
    set connector-source {string}
    set id {integer}
  next
end
```

config user adgrp

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 511	
server-name	FSSO agent name.	string	Maximum length: 35	
connector-source	FSSO connector source.	string	Maximum length: 35	
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config user certificate

Configure certificate users.

```
config user certificate
  Description: Configure certificate users.
  edit <name>
    set id {integer}
    set status [enable|disable]
    set type [single-certificate|trusted-issuer]
    set common-name {string}
    set issuer {string}
  next
end
```

config user certificate

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 64	
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
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.									
common-name	Certificate common name.	string	Maximum length: 64							
issuer	CA certificate used for client certificate verification.	string	Maximum length: 79							

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 hostname {string}
        set username {string}
        set password {password}
        set ip-address {ipv4-address}
        set ip6 {ipv6-address}
        set port {integer}
        set source-ip-address {ipv4-address}
        set source-ip6 {ipv6-address}
        set source-port {integer}
        set interface-select-method [auto|specify]
        set interface {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
set domain-name {string}
set domain-name-src [server|client]
set replication-port {integer}
set ldap-server <name1>, <name2>, ...
set change-detection [enable|disable]
set change-detection-period {integer}
set dns-srv-lookup [enable|disable]
set adlds-dn {string}
set adlds-ip-address {ipv4-address}
set adlds-ip6 {ipv6-address}
set adlds-port {integer}
next
end

```

config user domain-controller

Parameter	Description	Type	Size	Default
name	Domain controller entry name.	string	Maximum length: 35	
ad-mode	Set Active Directory mode.	option	-	none
	Option	Description		
	none	The server is not configured as an Active Directory Domain Server (AD DS).		
	ds	The server is configured as an Active Directory Domain Server (AD DS).		
	lds	The server is an Active Directory Lightweight Domain Server (AD LDS).		
hostname	Hostname of the server to connect to.	string	Maximum length: 255	
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64	
password	Password for specified username.	password	Not Specified	
ip-address	Domain controller IPv4 address.	ipv4-address	Not Specified	0.0.0.0
ip6	Domain controller IPv6 address.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default						
port	Port to be used for communication with the domain controller (default = 445).	integer	Minimum value: 0 Maximum value: 65535	445						
source-ip-address	FortiProxy IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	FortiProxy 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						
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
domain-name	Domain DNS name.	string	Maximum length: 255							
domain-name-src	Select where to extract domain name (default = server).	option	-	client						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>server</i></td><td>Extract domain name from server's (Domain Controller) data.</td></tr><tr><td><i>client</i></td><td>Extract domain name from client's data.</td></tr></table>				Option	Description	<i>server</i>	Extract domain name from server's (Domain Controller) data.	<i>client</i>	Extract domain name from client's data.
Option	Description									
<i>server</i>	Extract domain name from server's (Domain Controller) data.									
<i>client</i>	Extract domain name from client's data.									
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						
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
change-detection	Enable/disable detection of a configuration change in the Active Directory server.	option	-	disable						
	<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.									
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						

config extra-server

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 1 Maximum value: 100	0

Parameter	Description	Type	Size	Default
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
source-ip-address	FortiProxy 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 server-name {string}
        set domain-name {string}
        set username {string}
        set password {password}
        set ip {ipv4-address-any}
        set connect-protocol [rpc-over-tcp|rpc-over-http|...]
        set validate-server-certificate [disable|enable]
        set auth-type [spnego|ntlm|...]
        set auth-level [connect|call|...]
        set http-auth-type [basic|ntlm]
        set ssl-min-proto-version [default|SSLv3|...]
        set auto-discover-kdc [enable|disable]
        set kdc-ip <ipv41>, <ipv42>, ...
    next
end

```

config user exchange

Parameter	Description	Type	Size	Default
name	MS Exchange server entry name.	string	Maximum length: 35	
server-name	MS Exchange server hostname.	string	Maximum length: 63	
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79	
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64	
password	Password for the specified username.	password	Not Specified	
ip	Server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-	rpc-over-https
	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.		
validate-server-certificate	Enable/disable exchange server certificate validation.	option	-	disable
	Option Description			
	<i>disable</i>	Disable validation of server certificate.		
	<i>enable</i>	Enable validation of server certificate.		
auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos
	Option Description			
	<i>spnego</i>	Negotiate authentication.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></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>ntlm</i>	NTLM authentication.	<i>kerberos</i>	Kerberos authentication.											
	Option	Description																
	<i>ntlm</i>	NTLM authentication.																
<i>kerberos</i>	Kerberos authentication.																	
auth-level	Authentication security level used for the RPC protocol layer.	option	-	privacy														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>connect</i></td><td>RPC authentication level 'connect'.</td></tr><tr><td><i>call</i></td><td>RPC authentication level 'call'.</td></tr><tr><td><i>packet</i></td><td>RPC authentication level 'packet'.</td></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>connect</i>	RPC authentication level 'connect'.	<i>call</i>	RPC authentication level 'call'.	<i>packet</i>	RPC authentication level 'packet'.	<i>integrity</i>	RPC authentication level 'integrity'.	<i>privacy</i>	RPC authentication level 'privacy'.					
	Option	Description																
	<i>connect</i>	RPC authentication level 'connect'.																
	<i>call</i>	RPC authentication level 'call'.																
	<i>packet</i>	RPC authentication level 'packet'.																
	<i>integrity</i>	RPC authentication level 'integrity'.																
<i>privacy</i>	RPC authentication level 'privacy'.																	
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.																	
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><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.																	
auto- discover- kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic discovery of KDC IP addresses.		
	<i>disable</i>	Disable automatic discovery of KDC IP addresses.		
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79	

config user external-identity-provider

Configure external identity provider.

```

config user external-identity-provider
  Description: Configure external identity provider.
  edit <name>
    set type {option}
    set version [v1.0|beta]
    set url {string}
    set user-attr-name {string}
    set group-attr-name {string}
    set port {integer}
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
    set server-identity-check [disable|enable]
    set timeout {integer}
  next
end

```

config user external-identity-provider

Parameter	Description	Type	Size	Default
name	External identity provider name.	string	Maximum length: 35	
type	External identity provider type.	option	-	
	Option	Description		
	<i>ms-graph</i>	Microsoft Graph server.		
version	External identity API version.	option	-	

Parameter	Description	Type	Size	Default						
	<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).									
url	External identity provider URL (e.g. "https://example.com:8080/api/v1").	string	Maximum length: 127							
user-attr-name	User attribute name in authentication query.	string	Maximum length: 63	userPrincipalName						
group-attr-name	Group attribute name in authentication query.	string	Maximum length: 63	id						
port	External identity provider service port number (0 to use default).	integer	Minimum value: 0 Maximum value: 65535	0						
source-ip	Use this IPv4/v6 address to connect to the external identity provider.	string	Maximum length: 63							
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
server-identity-check	Enable/disable server's identity check against its certificate and subject alternative name(s).	option	-	enable						
	<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).									
timeout	Connection timeout value in seconds (default=5).	integer	Minimum value: 1 Maximum value: 60	5						

config user fortitoken

Configure FortiToken.

```
config user fortitoken
  Description: Configure FortiToken.
  edit <serial-number>
    set status [active|lock]
    set seed {string}
    set comments {var-string}
    set license {string}
    set activation-code {string}
    set activation-expire {integer}
    set reg-id {string}
    set os-ver {string}
  next
end
```

config user fortitoken

Parameter	Description	Type	Size	Default
serial-number	Serial number.	string	Maximum length: 16	
status	Status.	option	-	active
	Option	Description		
	<i>active</i>	Activate FortiToken.		
	<i>lock</i>	Lock FortiToken.		
seed	Token seed.	string	Maximum length: 208	
comments	Comment.	var-string	Maximum length: 255	
license	Mobile token license.	string	Maximum length: 31	
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	0

Parameter	Description	Type	Size	Default
reg-id	Device Reg ID.	string	Maximum length: 256	
os-ver	Device Mobile Version.	string	Maximum length: 15	

config user fsso

Configure Fortinet Single Sign On (FSSO) agents.

```

config user fsso
  Description: Configure Fortinet Single Sign On (FSSO) agents.
  edit <name>
    set type [default|fortinac]
    set server {string}
    set port {integer}
    set password {password}
    set server2 {string}
    set port2 {integer}
    set password2 {password}
    set server3 {string}
    set port3 {integer}
    set password3 {password}
    set server4 {string}
    set port4 {integer}
    set password4 {password}
    set server5 {string}
    set port5 {integer}
    set password5 {password}
    set logon-timeout {integer}
    set ldap-server {string}
    set group-poll-interval {integer}
    set ldap-poll [enable|disable]
    set ldap-poll-interval {integer}
    set ldap-poll-filter {string}
    set user-info-server {string}
    set ssl [enable|disable]
    set sni {string}
    set ssl-server-host-ip-check [enable|disable]
    set ssl-trusted-cert {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set interface-select-method [auto|specify]
    set interface {string}
  next
end

```

config user fsso

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Server type.	option	-	default
	Option	Description		
	<i>default</i>	All other unspecified types of servers.		
	<i>fortinac</i>	FortiNAC server.		
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63	
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password	Password of the first FSSO collector agent.	password	Not Specified	
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63	
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password2	Password of the second FSSO collector agent.	password	Not Specified	
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63	
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password3	Password of the third FSSO collector agent.	password	Not Specified	

Parameter	Description	Type	Size	Default
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63	
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password4	Password of the fourth FSSO collector agent.	password	Not Specified	
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63	
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password5	Password of the fifth FSSO collector agent.	password	Not Specified	
logon-timeout	Interval in minutes to keep logons after FSSO server down.	integer	Minimum value: 1 Maximum value: 2880	5
ldap-server	LDAP server to get group information.	string	Maximum length: 35	
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
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-	disable
	Option	Description		
	enable	Enable automatic fetching of groups from LDAP server.		
	disable	Disable automatic fetching of groups from LDAP server.		

Parameter	Description	Type	Size	Default						
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180						
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047	(objectCategory=group)						
user-info-server	LDAP server to get user information.	string	Maximum length: 35							
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.									
sni	Server Name Indication.	string	Maximum length: 255							
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							
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	::						
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></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.		
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

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>
    set status [enable|disable]
    set server {string}
    set default-domain {string}
    set port {integer}
    set user {string}
    set password {password}
    set ldap-server {string}
    set logon-history {integer}
    set polling-frequency {integer}
    config adgrp
      Description: LDAP Group Info.
      edit <name>
        next
      end
    end
    set smbv1 [enable|disable]
    set smb-ntlmv1-auth [enable|disable]
  next
end

```

config user fsso-polling

Parameter	Description	Type	Size	Default
id	Active Directory server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable polling for the status of this Active Directory server.	option	-	enable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63	
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35	
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535	0
user	User name required to log into this Active Directory server.	string	Maximum length: 35	
password	Password required to log into this Active Directory server.	password	Not Specified	
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
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30	10
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.		
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.		

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 id {integer}
    set group-type [firewall|fsso-service|...]
    set authtimeout {integer}
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set http-digest-realm {string}
    set sso-attribute-value {string}
    set logic-type [or|and]
    set member <name1>, <name2>, ...
  config match
    Description: Group matches.
    edit <id>
      set server-name {string}
      set group-name {string}
    next
  end
  set user-id [email|auto-generate|...]
  set password [auto-generate|specify|...]
  set user-name [disable|enable]
  set sponsor [optional|mandatory|...]
  set company [optional|mandatory|...]
  set email [disable|enable]
  set mobile-phone [disable|enable]
  set sms-server [fortiguard|custom]
  set sms-custom-server {string}
  set expire-type [immediately|first-successful-login]
  set expire {integer}
  set max-accounts {integer}
  set multiple-guest-add [disable|enable]
  config guest
    Description: Guest User.
    edit <id>
      set user-id {string}
      set name {string}
      set password {password}
      set mobile-phone {string}
```

```

        set sponsor {string}
        set company {string}
        set email {string}
        set expiration {user}
        set comment {var-string}
    next
end
next
end

```

config user group

Parameter	Description	Type	Size	Default										
name	Group name.	string	Maximum length: 35											
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-	firewall										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>firewall</td><td>Firewall.</td></tr><tr><td>fsso-service</td><td>Fortinet Single Sign-On Service.</td></tr><tr><td>rsso</td><td>RADIUS based Single Sign-On Service.</td></tr><tr><td>guest</td><td>Guest.</td></tr></table>				Option	Description	firewall	Firewall.	fsso-service	Fortinet Single Sign-On Service.	rsso	RADIUS based Single Sign-On Service.	guest	Guest.
Option	Description													
firewall	Firewall.													
fsso-service	Fortinet Single Sign-On Service.													
rsso	RADIUS based Single Sign-On Service.													
guest	Guest.													
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 Maximum value: 43200	0										
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable auth-concurrent-override.</td></tr><tr><td>disable</td><td>Disable auth-concurrent-override.</td></tr></table>				Option	Description	enable	Enable auth-concurrent-override.	disable	Disable auth-concurrent-override.				
Option	Description													
enable	Enable auth-concurrent-override.													
disable	Disable auth-concurrent-override.													

Parameter	Description	Type	Size	Default								
auth-concurrent-value	Maximum number of concurrent authenticated connections per user (0 - 100).	integer	Minimum value: 0 Maximum value: 100	0								
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35									
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511									
logic-type	Set the logic between members or matching entries.	option	-	or								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>or</i></td><td>Logic OR between members or match entries.</td></tr><tr><td><i>and</i></td><td>Logic AND between members or match entries.</td></tr></table>				Option	Description	<i>or</i>	Logic OR between members or match entries.	<i>and</i>	Logic AND between members or match entries.		
Option	Description											
<i>or</i>	Logic OR between members or match entries.											
<i>and</i>	Logic AND between members or match entries.											
member <name>	Names of users, peers, LDAP servers, RADIUS servers or external idp servers to add to the user group. Group member name.	string	Maximum length: 511									
user-id	Guest user ID type.	option	-	email								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email</i></td><td>Email address.</td></tr><tr><td><i>auto-generate</i></td><td>Automatically generate.</td></tr><tr><td><i>specify</i></td><td>Specify.</td></tr></table>				Option	Description	<i>email</i>	Email address.	<i>auto-generate</i>	Automatically generate.	<i>specify</i>	Specify.
Option	Description											
<i>email</i>	Email address.											
<i>auto-generate</i>	Automatically generate.											
<i>specify</i>	Specify.											
password	Guest user password type.	option	-	auto-generate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-generate</i></td><td>Automatically generate.</td></tr><tr><td><i>specify</i></td><td>Specify.</td></tr><tr><td><i>disable</i></td><td>Disable.</td></tr></table>				Option	Description	<i>auto-generate</i>	Automatically generate.	<i>specify</i>	Specify.	<i>disable</i>	Disable.
Option	Description											
<i>auto-generate</i>	Automatically generate.											
<i>specify</i>	Specify.											
<i>disable</i>	Disable.											
user-name	Enable/disable the guest user name entry.	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.											

Parameter	Description	Type	Size	Default								
sponsor	Set the action for the sponsor guest user field.	option	-	optional								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Optional.</td></tr><tr><td><i>mandatory</i></td><td>Mandatory.</td></tr><tr><td><i>disabled</i></td><td>Disabled.</td></tr></table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
Option	Description											
<i>optional</i>	Optional.											
<i>mandatory</i>	Mandatory.											
<i>disabled</i>	Disabled.											
company	Set the action for the company guest user field.	option	-	optional								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Optional.</td></tr><tr><td><i>mandatory</i></td><td>Mandatory.</td></tr><tr><td><i>disabled</i></td><td>Disabled.</td></tr></table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
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								
	<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.											
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.											
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.					
Option	Description											
<i>fortiguard</i>	Send SMS by FortiGuard.											
<i>custom</i>	Send SMS by custom server.											
sms-custom-server	SMS server.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
expire-type	Determine when the expiration countdown begins.	option	-	immediately						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediately</i></td><td>Immediately.</td></tr><tr><td><i>first-successful-login</i></td><td>First successful login.</td></tr></table>				Option	Description	<i>immediately</i>	Immediately.	<i>first-successful-login</i>	First successful login.
Option	Description									
<i>immediately</i>	Immediately.									
<i>first-successful-login</i>	First successful login.									
expire	Time in seconds before guest user accounts expire (1 - 31536000).	integer	Minimum value: 1 Maximum value: 31536000	14400						
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 1024	0						
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.									

config match

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-name	Name of remote auth server.	string	Maximum length: 35	
group-name	Name of matching user or group on remote authentication server.	string	Maximum length: 511	

config guest

Parameter	Description	Type	Size	Default
id	Guest ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
user-id	Guest ID.	string	Maximum length: 64	
name	Guest name.	string	Maximum length: 64	
password	Guest password.	password	Not Specified	
mobile-phone	Mobile phone.	string	Maximum length: 35	
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35	
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	
comment	Comment.	var-string	Maximum length: 255	

config user krb-keytab

Configure Kerberos keytab entries.

```
config user krb-keytab
  Description: Configure Kerberos keytab entries.
  edit <name>
    set pac-data [enable|disable]
    set principal {string}
    set ldap-server <name1>, <name2>, ...
    set keytab {string}
  next
end
```

config user krb-keytab

Parameter	Description	Type	Size	Default
name	Kerberos keytab entry name.	string	Maximum length: 35	
pac-data	Enable/disable parsing PAC data in the ticket.	option	-	enable
	Option	Description		
	enable	Enable parsing PAC data in the ticket.		
	disable	Disable parsing PAC data in the ticket.		
principal	Kerberos service principal. For example, HTTP/myfgt.example.com@example.com.	string	Maximum length: 511	
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79	
keytab	Base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191	

config user ldap

Configure LDAP server entries.

```
config user ldap
  Description: Configure LDAP server entries.
  edit <name>
    set server {string}
    set secondary-server {string}
    set tertiary-server {string}
    set status-ttl {integer}
    set server-identity-check [enable|disable]
    set source-ip {string}
    set source-port {integer}
    set cnid {string}
    set dn {string}
    set type [simple|anonymous|...]
    set two-factor [disable|fortitoken-cloud]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set two-factor-filter {string}
    set username {string}
    set password {password}
    set group-member-check [user-attr|group-object|...]
    set group-search-base {string}
    set group-object-filter {string}
```

```

set group-filter {string}
set secure [disable|starttls|...]
set ssl-max-proto-version [SSLv3|TLSv1|...]
set ssl-min-proto-version [default|SSLv3|...]
set ca-cert {string}
set port {integer}
set password-expiry-warning [enable|disable]
set password-renewal [enable|disable]
set member-attr {string}
set account-key-processing [same|strip]
set account-key-cert-field [othername|rfc822name|...]
set account-key-filter {string}
set search-type {option1}, {option2}, ...
set max-connections {integer}
set client-cert-auth [enable|disable]
set client-cert {string}
set obtain-user-info [enable|disable]
set user-info-exchange-server {string}
set interface-select-method [auto|specify]
set interface {string}
set antiphish [enable|disable]
set password-attr {string}
next
end

```

config user ldap

Parameter	Description	Type	Size	Default
name	LDAP server entry name.	string	Maximum length: 35	
server	LDAP server CN domain name or IP.	string	Maximum length: 63	
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63	
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
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						
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	FortiProxy IP address to be used for communication with the LDAP server.	string	Maximum length: 63							
source-port	Source port to be used for communication with the LDAP server.	integer	Minimum value: 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default								
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									
type	Authentication type for LDAP searches.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple password authentication without search.</td></tr><tr><td><i>anonymous</i></td><td>Bind using anonymous user search.</td></tr><tr><td><i>regular</i></td><td>Bind using username/password and then search.</td></tr></table>				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.
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.											
two-factor	Enable/disable two-factor authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable two-factor authentication.</td></tr><tr><td><i>fortitoken-cloud</i></td><td>FortiToken Cloud Service.</td></tr></table>				Option	Description	<i>disable</i>	disable two-factor authentication.	<i>fortitoken-cloud</i>	FortiToken Cloud Service.		
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-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.		
two-factor-filter	Filter used to synchronize users to FortiToken Cloud.	string	Maximum length: 2047	
username	Username (full DN) for initial binding.	string	Maximum length: 511	
password	Password for initial binding.	password	Not Specified	
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-search-base	Search base used for group searching.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
group-object-filter	Filter used for group searching.	string	Maximum length: 2047	(&(objectcategory=group)(member=*))
group-filter	Filter used for group matching.	string	Maximum length: 2047	
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.	
ssl-max-version	Maximum supported protocol version for SSL/TLS connections.	option	-	TLSv1-3
	Option		Description	
	<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.	
ssl-min-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.		
ca-cert	CA certificate name.	string	Maximum length: 79	
port	Port to be used for communication with the LDAP server (default = 389).	integer	Minimum value: 1 Maximum value: 65535	389
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable
	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.		

Parameter	Description	Type	Size	Default										
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf										
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.													
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-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)))										
search-type	Search type.	option	-	recursive										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.		
max-connections	Maximum LDAP server connections (16-5000, default 64).	integer	Minimum value: 16 Maximum value: 5000	64
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.		
client-cert	Client certificate name.	string	Maximum length: 79	
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable obtaining of user information.		
	<i>disable</i>	Disable obtaining of user information.		
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
antiphish	Enable/disable AntiPhishing credential backend.	option	-	disable
	Option	Description		
	enable	Enable AntiPhishing credential backend.		
	disable	Disable AntiPhishing credential backend.		
password-attr	Name of attribute to get password hash.	string	Maximum length: 35	userPassword

config user local

Configure local users.

```

config user local
  Description: Configure local users.
  edit <name>
    set id {integer}
    set status [enable|disable]
    set type [password|radius|...]
    set passwd {password}
    set ldap-server {string}
    set radius-server {string}
    set tacacs+-server {string}
    set two-factor [disable|fortitoken|...]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set fortitoken {string}
    set email-to {string}
    set sms-server [fortiguard|custom]
    set sms-custom-server {string}

```

```

set sms-phone {string}
set passwd-policy {string}
set passwd-time {user}
set authtimeout {integer}
set workstation {string}
set auth-concurrent-override [enable|disable]
set auth-concurrent-value {integer}
set ppk-secret {password-3}
set ppk-identity {string}
set qkd-profile {string}
set username-sensitivity [disable|enable]
next
end

```

config user local

Parameter	Description	Type	Size	Default										
name	Local user name.	string	Maximum length: 64											
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
status	Enable/disable allowing the local user to authenticate with the FortiProxy 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	Authentication method.	option	-	password										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>password</i></td><td>Password authentication.</td></tr><tr><td><i>radius</i></td><td>RADIUS server authentication.</td></tr><tr><td><i>tacacs+</i></td><td>TACACS+ server authentication.</td></tr><tr><td><i>ldap</i></td><td>LDAP server authentication.</td></tr></table>				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.
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.													
passwd	User's password.	password	Not Specified											
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35											

Parameter	Description	Type	Size	Default												
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35													
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><i>disable</i></td><td>disable</td></tr><tr><td><i>fortitoken</i></td><td>FortiToken</td></tr><tr><td><i>fortitoken-cloud</i></td><td>FortiToken Cloud Service.</td></tr><tr><td><i>email</i></td><td>Email authentication code.</td></tr><tr><td><i>sms</i></td><td>SMS authentication code.</td></tr></table>	Option	Description	<i>disable</i>	disable	<i>fortitoken</i>	FortiToken	<i>fortitoken-cloud</i>	FortiToken Cloud Service.	<i>email</i>	Email authentication code.	<i>sms</i>	SMS authentication code.			
	Option	Description														
	<i>disable</i>	disable														
	<i>fortitoken</i>	FortiToken														
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.														
	<i>email</i>	Email authentication code.														
<i>sms</i>	SMS authentication code.															
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.															
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16													
email-to	Two-factor recipient's email address.	string	Maximum length: 63													
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard												

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>				Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.
	Option	Description								
	<i>fortiguard</i>	Send SMS by FortiGuard.								
<i>custom</i>	Send SMS by custom server.									
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							
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							
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440	0						
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							
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.									
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100	0						
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35							
qkd-profile	Quantum Key Distribution (QKD) profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default	
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.		

config user oidc

Configure OpenID Connect servers.

```

config user oidc
  Description: Configure OpenID Connect servers.
  edit <name>
    set display-name {string}
    set icon-url {string}
    set type [discovery|manual]
    set client-id {string}
    set auth-type [client-secret|private-key]
    set auth-method [client_secret_basic|client_secret_post|...]
    set client-secret {string}
    set private-key {string}
    set verify-cert [enable|disable]
    set discovery-url {string}
    set authorization-url {string}
    set token-url {string}
    set jwks-uri {string}
    set domain-hint {string}
    set issuer {string}
    set verify-issuer [enable|disable]
    set user-attr-name [email|sub|...]
    set user-regex {string}
    set group-attr-name {string}
    set ldap-server <name1>, <name2>, ...
    set clock-tolerance {integer}
  next
end

```


config user oidc

Parameter	Description	Type	Size	Default
name	OpenID Connect server entry name.	string	Maximum length: 35	
display-name	Display name. Used in OpenID Connect landing page.	string	Maximum length: 35	
icon-url	Icon URL. Used in OpenID Connect landing page.	string	Maximum length: 255	
type	Type of OpenID Connect config.	option	-	discovery
	Option		Description	
	<i>discovery</i>	Use discovery URL to get configuration.		
	<i>manual</i>	Use manual configuration.		
client-id	OpenID Connect server client ID.	string	Maximum length: 127	
auth-type	Authentication Type of OpenID Connect config.	option	-	client-secret
	Option		Description	
	<i>client-secret</i>	Authorization with Client Secret.		
	<i>private-key</i>	Authorization with RSA Private Key.		
auth-method	Client Authentication method for Token Endpoint.	option	-	client_secret_basic
	Option		Description	
	<i>client_secret_basic</i>	Authorization using the HTTP Basic Authentication scheme.		
	<i>client_secret_post</i>	Authorization by including client credentials in the request body.		
	<i>private_key_jwt</i>	Authorization using the JWT profile and Assertion Framework for OAuth 2.0.		
client-secret	OpenID Connect server client secret.	string	Maximum length: 255	
private-key	OpenID Connect server RSA private key.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
verify-cert	Enable/disable certificate verification (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		
discovery-url	OpenID Connect server discovery URL.	string	Maximum length: 255	
authorization-url	OpenID Connect server authorization URL.	string	Maximum length: 255	
token-url	OpenID Connect server token URL.	string	Maximum length: 255	
jwt-uri	URL of the OP's JWK Set document.	string	Maximum length: 255	
domain-hint	Domain Hint.	string	Maximum length: 255	
issuer	OpenID Connect server issuer.	string	Maximum length: 255	
verify-issuer	Verify issuer in ID token (default = enable).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable verification of issuer in ID token (default).		
	<i>disable</i>	Disable verification of issuer in ID token.		
user-attr-name	Which field in ID token is username	option	-	email
	Option	Description		
	<i>email</i>	Use email in ID token as username.		
	<i>sub</i>	Use sub in ID token as username.		
	<i>preferred_username</i>	Use preferred_username in ID token as username.		
user-regex	username must match this regex (case insensitive).	string	Maximum length: 255	
group-attr-name	Which field in ID token is group names	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79	
clock-tolerance	Clock skew tolerance in seconds (0 - 300, default = 15, 0 = no tolerance).	integer	Minimum value: 0 Maximum value: 300	15

config user password-policy

Configure user password policy.

```

config user password-policy
  Description: Configure user password policy.
  edit <name>
    set expire-days {integer}
    set warn-days {integer}
    set expired-password-renewal [enable|disable]
    set minimum-length {integer}
    set min-lower-case-letter {integer}
    set min-upper-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-change-characters {integer}
    set expire-status [enable|disable]
    set reuse-password [enable|disable]
  next
end

```

config user password-policy

Parameter	Description	Type	Size	Default
name	Password policy name.	string	Maximum length: 35	
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180
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

Parameter	Description	Type	Size	Default						
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.									
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase 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						
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-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						
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.									

Parameter	Description	Type	Size	Default
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable
	Option	Description		
	<i>enable</i>	Users are allowed to reuse the same password.		
	<i>disable</i>	Users must create a new password.		

config user peer

Configure peer users.

```

config user peer
  Description: Configure peer users.
  edit <name>
    set mandatory-ca-verify [enable|disable]
    set ca {string}
    set subject {string}
    set cn {string}
    set cn-type [string|email|...]
    set mfa-mode [none|password|...]
    set mfa-server {string}
    set mfa-username {string}
    set mfa-password {password}
    set ocsf-override-server {string}
    set two-factor [enable|disable]
    set passwd {password}
  next
end

```

config user peer

Parameter	Description	Type	Size	Default
name	Peer name.	string	Maximum length: 35	
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

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.															
ca	Name of the CA certificate.	string	Maximum length: 127													
subject	Peer certificate name constraints.	string	Maximum length: 255													
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.															
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-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													
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													

Parameter	Description	Type	Size	Default
ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35	
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable 2-factor authentication.		
	<i>disable</i>	Disable 2-factor authentication.		
passwd	Peer's password used for two-factor authentication.	password	Not Specified	

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
name	Peer group name.	string	Maximum length: 35	
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	

config user pop3

POP3 server entry configuration.

```
config user pop3
    Description: POP3 server entry configuration.
    edit <name>
```

```

    set server {string}
    set port {integer}
    set secure [none|starttls|...]
    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															
server	Server domain name or IP address.	string	Maximum length: 63															
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><i>none</i></td><td>None.</td></tr><tr><td><i>starttls</i></td><td>Use StartTLS.</td></tr><tr><td><i>pop3s</i></td><td>Use POP3 over SSL.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>starttls</i>	Use StartTLS.	<i>pop3s</i>	Use POP3 over SSL.									
Option	Description																	
<i>none</i>	None.																	
<i>starttls</i>	Use StartTLS.																	
<i>pop3s</i>	Use POP3 over SSL.																	
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.																	

config user radius

Configure RADIUS server entries.

```
config user radius
  Description: Configure RADIUS server entries.
  edit <name>
    set server {string}
    set secret {password}
    set secondary-server {string}
    set secondary-secret {password}
    set tertiary-server {string}
    set tertiary-secret {password}
    set timeout {integer}
    set status-ttl {integer}
    set all-usergroup [disable|enable]
    set use-management-vdom [enable|disable]
    set nas-ip {ipv4-address}
    set nas-id-type [legacy|custom|...]
    set call-station-id-type [legacy|IP|...]
    set nas-id {string}
    set acct-interim-interval {integer}
    set radius-coa [enable|disable]
    set radius-port {integer}
    set h3c-compatibility [enable|disable]
    set auth-type [auto|ms_chap_v2|...]
    set source-ip {string}
    set username-case-sensitive [enable|disable]
    set group-override-attr-type [filter-Id|class]
    set class <name1>, <name2>, ...
    set password-renewal [enable|disable]
    set require-message-authenticator [enable|disable]
    set password-encoding [auto|ISO-8859-1]
    set mac-username-delimiter [hyphen|single-hyphen|...]
    set mac-password-delimiter [hyphen|single-hyphen|...]
    set mac-case [uppercase|lowercase]
    set acct-all-servers [enable|disable]
    set switch-controller-acct-fast-framedip-detect {integer}
    set interface-select-method [auto|specify]
    set interface {string}
    set switch-controller-service-type {option1}, {option2}, ...
    set transport-protocol [udp|tcp|...]
    set tls-min-proto-version [default|SSLv3|...]
    set ca-cert {string}
    set client-cert {string}
    set server-identity-check [enable|disable]
    set account-key-processing [same|strip]
    set account-key-cert-field [othername|rfc822name|...]
    set rso [enable|disable]
    set rso-radius-server-port {integer}
    set rso-radius-response [enable|disable]
```

```

set rso-validate-request-secret [enable|disable]
set rso-secret {password}
set rso-endpoint-attribute [User-Name|NAS-IP-Address|...]
set rso-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute-key {string}
set sso-attribute-value-override [enable|disable]
set rso-context-timeout {integer}
set rso-log-period {integer}
set rso-log-flags {option1}, {option2}, ...
set rso-flush-ip-session [enable|disable]
set rso-ep-one-ip-only [enable|disable]
set delimiter [plus|comma]
config accounting-server
    Description: Additional accounting servers.
    edit <id>
        set status [enable|disable]
        set server {string}
        set secret {password}
        set port {integer}
        set source-ip {string}
        set interface-select-method [auto|specify]
        set interface {string}
    next
end
next
end

```

config user radius

Parameter	Description	Type	Size	Default
name	RADIUS server entry name.	string	Maximum length: 35	
server	Primary RADIUS server 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	
secondary-server	Secondary RADIUS CN domain name or IP address.	string	Maximum length: 63	
secondary-secret	Secret key to access the secondary server.	password	Not Specified	
tertiary-server	Tertiary RADIUS CN domain name or IP address.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default								
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified									
timeout	Time in seconds to retry connecting server.	integer	Minimum value: 1 Maximum value: 300	5								
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								
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not automatically include this server in a user group.</td></tr><tr><td><i>enable</i></td><td>Include this RADIUS server in every user group.</td></tr></table>				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.		
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.											
use-management-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>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.											
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								
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.											

Parameter	Description	Type	Size	Default								
call-station-id-type	Calling & Called station identifier type configuration (default = legacy), this option is not available for 802.1x authentication.	option	-	legacy								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>legacy</td><td>Calling & Called station identifier is the value previously used by each daemon.</td></tr><tr><td>IP</td><td>Calling & Called station identifier is the value of IP address.</td></tr><tr><td>MAC</td><td>Calling & Called station identifier is the value of MAC address.</td></tr></table>	Option	Description	legacy	Calling & Called station identifier is the value previously used by each daemon.	IP	Calling & Called station identifier is the value of IP address.	MAC	Calling & Called station identifier is the value of MAC address.			
Option	Description											
legacy	Calling & Called station identifier is the value previously used by each daemon.											
IP	Calling & Called station identifier is the value of IP address.											
MAC	Calling & Called station identifier is the value of MAC address.											
nas-id	Custom NAS identifier.	string	Maximum length: 255									
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 60 Maximum value: 86400	0								
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 Maximum value: 65535	0								
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>enable</td><td>Enable H3C compatibility.</td></tr><tr><td>disable</td><td>Disable H3C compatibility.</td></tr></table>	Option	Description	enable	Enable H3C compatibility.	disable	Disable H3C compatibility.					
Option	Description											
enable	Enable H3C compatibility.											
disable	Disable H3C compatibility.											

Parameter	Description	Type	Size	Default												
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Use PAP, MSCHAP_v2, and CHAP (in that order).</td></tr><tr><td>ms_chap_v2</td><td>Microsoft Challenge Handshake Authentication Protocol version 2.</td></tr><tr><td>ms_chap</td><td>Microsoft Challenge Handshake Authentication Protocol.</td></tr><tr><td>chap</td><td>Challenge Handshake Authentication Protocol.</td></tr><tr><td>pap</td><td>Password Authentication Protocol.</td></tr></table>	Option	Description	auto	Use PAP, MSCHAP_v2, and CHAP (in that order).	ms_chap_v2	Microsoft Challenge Handshake Authentication Protocol version 2.	ms_chap	Microsoft Challenge Handshake Authentication Protocol.	chap	Challenge Handshake Authentication Protocol.	pap	Password Authentication Protocol.			
Option	Description															
auto	Use PAP, MSCHAP_v2, and CHAP (in that order).															
ms_chap_v2	Microsoft Challenge Handshake Authentication Protocol version 2.															
ms_chap	Microsoft Challenge Handshake Authentication Protocol.															
chap	Challenge Handshake Authentication Protocol.															
pap	Password Authentication Protocol.															
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63													
username-case-sensitive	Enable/disable case sensitive user names.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable username case-sensitive.</td></tr><tr><td>disable</td><td>Disable username case-sensitive.</td></tr></table>	Option	Description	enable	Enable username case-sensitive.	disable	Disable username case-sensitive.									
Option	Description															
enable	Enable username case-sensitive.															
disable	Disable username case-sensitive.															
group-override-attr-type	RADIUS attribute type to override user group information.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>filter-Id</td><td>Filter-Id</td></tr><tr><td>class</td><td>Class</td></tr></table>	Option	Description	filter-Id	Filter-Id	class	Class									
Option	Description															
filter-Id	Filter-Id															
class	Class															
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79													
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.															

Parameter	Description	Type	Size	Default										
require-message-authenticator	Require message authenticator in authentication response.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Make the validation of message authenticator mandatory in authentication response.</td></tr><tr><td><i>disable</i></td><td>Make the validation of message authenticator optional in authentication response.</td></tr></table>	Option	Description	<i>enable</i>	Make the validation of message authenticator mandatory in authentication response.	<i>disable</i>	Make the validation of message authenticator optional in authentication response.							
Option	Description													
<i>enable</i>	Make the validation of message authenticator mandatory in authentication response.													
<i>disable</i>	Make the validation of message authenticator optional in authentication response.													
password-encoding	Password encoding.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Use original password encoding.</td></tr><tr><td><i>ISO-8859-1</i></td><td>Use ISO-8859-1 password encoding.</td></tr></table>	Option	Description	<i>auto</i>	Use original password encoding.	<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.							
Option	Description													
<i>auto</i>	Use original password encoding.													
<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.													
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.													
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-case	MAC authentication case (default = lowercase).	option	-	lowercase										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>uppercase</i>	Use uppercase MAC.		
	<i>lowercase</i>	Use lowercase MAC.		
acct-all-servers	Enable/disable sending of accounting messages to all configured servers (default = disable).	option	-	disable
	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.		
switch-controller-acct-fast-framedip-detect	Switch controller accounting message Framed-IP detection from DHCP snooping (seconds, default=2).	integer	Minimum value: 2 Maximum value: 600	2
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
switch-controller-service-type	RADIUS service type.	option	-	
	Option	Description		
	<i>login</i>	User should be connected to a host.		
	<i>framed</i>	User use Framed Protocol.		
	<i>callback-login</i>	User disconnected and called back.		
	<i>callback-framed</i>	User disconnected and called back, then a Framed Protocol.		
	<i>outbound</i>	User granted access to outgoing devices.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>administrative</i></td><td>User granted access to the administrative unsigned interface.</td></tr><tr><td><i>nas-prompt</i></td><td>User provided a command prompt on the NAS.</td></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>administrative</i>	User granted access to the administrative unsigned interface.	<i>nas-prompt</i>	User provided a command prompt on the NAS.	<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>administrative</i>	User granted access to the administrative unsigned interface.																
	<i>nas-prompt</i>	User provided a command prompt on the NAS.																
	<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.																	
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.																	
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.																	
ca-cert	CA of server to trust under TLS.	string	Maximum length: 79															
client-cert	Client certificate to use under TLS.	string	Maximum length: 35															

Parameter	Description	Type	Size	Default										
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.													
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><i>same</i></td><td>Same as subject identity field.</td></tr><tr><td><i>strip</i></td><td>Strip domain string from subject identity field.</td></tr></table>	Option	Description	<i>same</i>	Same as subject identity field.	<i>strip</i>	Strip domain string from subject identity field.							
Option	Description													
<i>same</i>	Same as subject identity field.													
<i>strip</i>	Strip domain string from subject identity field.													
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><i>othername</i></td><td>Other name in SAN.</td></tr><tr><td><i>rfc822name</i></td><td>RFC822 email address in SAN.</td></tr><tr><td><i>dnsname</i></td><td>DNS name in SAN.</td></tr><tr><td><i>cn</i></td><td>CN in subject.</td></tr></table>	Option	Description	<i>othername</i>	Other name in SAN.	<i>rfc822name</i>	RFC822 email address in SAN.	<i>dnsname</i>	DNS name in SAN.	<i>cn</i>	CN in subject.			
Option	Description													
<i>othername</i>	Other name in SAN.													
<i>rfc822name</i>	RFC822 email address in SAN.													
<i>dnsname</i>	DNS name in SAN.													
<i>cn</i>	CN in subject.													
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS based single sign on feature.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS based single sign on feature.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS based single sign on feature.	<i>disable</i>	Disable RADIUS based single sign on feature.							
Option	Description													
<i>enable</i>	Enable RADIUS based single sign on feature.													
<i>disable</i>	Disable RADIUS based single sign on feature.													
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 0 Maximum value: 65535	1813										

Parameter	Description	Type	Size	Default
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sending RADIUS response packets.		
	<i>disable</i>	Disable sending RADIUS response packets.		
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable validating RADIUS request shared secret.		
	<i>disable</i>	Disable validating RADIUS request shared secret.		
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified	
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.			

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></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-LA T-Service</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LA T-Node</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LA T-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-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-LA T-Service</i>	Use this attribute.	<i>Login-LA T-Node</i>	Use this attribute.	<i>Login-LA T-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-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-LA T-Service</i>	Use this attribute.																												
	<i>Login-LA T-Node</i>	Use this attribute.																												
	<i>Login-LA T-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.																													
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-																											
	<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><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></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.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</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.																												
<i>Framed-IP-Netmask</i>	Use this attribute.																													
<i>Filter-Id</i>	Use this attribute.																													

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></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>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>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	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-	Class																																				

Parameter	Description	Type	Size	Default
	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.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></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>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.			
	Option	Description								
	<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							
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable override old attribute value with new value for the same endpoint.</td></tr><tr><td><i>disable</i></td><td>Disable override old attribute value with new value for the same endpoint.</td></tr></table>	Option	Description	<i>enable</i>	Enable override old attribute value with new value for the same endpoint.	<i>disable</i>	Disable override old attribute value with new value for the same endpoint.			
	Option	Description								
	<i>enable</i>	Enable override old attribute value with new value for the same endpoint.								
<i>disable</i>	Disable override old attribute value with new value for the same endpoint.									
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-log-period	Time interval in seconds that group event log messages will be generated for dynamic profile events.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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><i>protocol-error</i></td><td>Enable this log type.</td></tr></table>	Option	Description	<i>protocol-error</i>	Enable this log type.					
	Option	Description								
<i>protocol-error</i>	Enable this log type.									

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>profile-missing</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-stop-missed</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-event</i></td><td>Enable this log type.</td></tr><tr><td><i>endpoint-block</i></td><td>Enable this log type.</td></tr><tr><td><i>radiusd-other</i></td><td>Enable this log type.</td></tr><tr><td><i>none</i></td><td>Disable all logging.</td></tr></table>	Option	Description	<i>profile-missing</i>	Enable this log type.	<i>accounting-stop-missed</i>	Enable this log type.	<i>accounting-event</i>	Enable this log type.	<i>endpoint-block</i>	Enable this log type.	<i>radiusd-other</i>	Enable this log type.	<i>none</i>	Disable all logging.			
	Option	Description																
	<i>profile-missing</i>	Enable this log type.																
	<i>accounting-stop-missed</i>	Enable this log type.																
	<i>accounting-event</i>	Enable this log type.																
	<i>endpoint-block</i>	Enable this log type.																
	<i>radiusd-other</i>	Enable this log type.																
<i>none</i>	Disable all logging.																	
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><i>enable</i></td><td>Enable flush user IP sessions on RADIUS accounting stop.</td></tr><tr><td><i>disable</i></td><td>Disable flush user IP sessions on RADIUS accounting stop.</td></tr></table>	Option	Description	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.	<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.											
	Option	Description																
	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.																
<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.																	
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><i>enable</i></td><td>Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr><tr><td><i>disable</i></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	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.	<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.											
	Option	Description																
	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																
<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																	
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 ",".																	

config accounting-server

Parameter	Description	Type	Size	Default						
id	ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
server	Server CN domain name or IP address.	string	Maximum length: 63							
secret	Secret key.	password	Not Specified							
port	RADIUS accounting port number.	integer	Minimum value: 0 Maximum value: 65535	0						
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63							
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config user saml

SAML server entry configuration.

```
config user saml
  Description: SAML server entry configuration.
  edit <name>
    set cert {string}
    set entity-id {string}
```



```

set single-sign-on-url {string}
set single-logout-url {string}
set idp-entity-id {string}
set idp-single-sign-on-url {string}
set idp-single-logout-url {string}
set idp-cert {string}
set user-name {string}
set group-name {string}
set digest-method [sha1|sha256]
set limit-relaystate [enable|disable]
set clock-tolerance {integer}
set adfs-claim [enable|disable]
set user-claim-type [email|given-name|...]
set group-claim-type [email|given-name|...]
set reauth [enable|disable]
next
end

```

config user saml

Parameter	Description	Type	Size	Default
name	SAML server entry name.	string	Maximum length: 35	
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
entity-id	SP entity ID.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
single-logout-url	SP single logout URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255	
idp-cert	IDP Certificate name.	string	Maximum length: 35	
user-name	User name in assertion statement.	string	Maximum length: 255	
group-name	Group name in assertion statement.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default												
digest-method	Digest method algorithm (default = sha1).	option	-	sha1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha1</td><td>Digest Method Algorithm is SHA1.</td></tr><tr><td>sha256</td><td>Digest Method Algorithm is SHA256.</td></tr></table>	Option	Description	sha1	Digest Method Algorithm is SHA1.	sha256	Digest Method Algorithm is SHA256.									
Option	Description															
sha1	Digest Method Algorithm is SHA1.															
sha256	Digest Method Algorithm is SHA256.															
limit-relaystate	Enable/disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr><tr><td>disable</td><td>Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr></table>	Option	Description	enable	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	disable	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).									
Option	Description															
enable	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).															
disable	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).															
clock-tolerance	Clock skew tolerance in seconds (0 - 300, default = 15, 0 = no tolerance).	integer	Minimum value: 0 Maximum value: 300	15												
adfs-claim	Enable/disable ADFS Claim for user/group attribute in assertion statement (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ADFS Claim for user/group attribute in assertion statement.</td></tr><tr><td>disable</td><td>Disable ADFS Claim for user/group attribute in assertion statement.</td></tr></table>	Option	Description	enable	Enable ADFS Claim for user/group attribute in assertion statement.	disable	Disable ADFS Claim for user/group attribute in assertion statement.									
Option	Description															
enable	Enable ADFS Claim for user/group attribute in assertion statement.															
disable	Disable ADFS Claim for user/group attribute in assertion statement.															
user-claim-type	User name claim in assertion statement.	option	-	upn												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>email</td><td>E-mail address of the user.</td></tr><tr><td>given-name</td><td>Given name of the user.</td></tr><tr><td>name</td><td>Unique name of the user.</td></tr><tr><td>upn</td><td>User principal name (UPN) of the user.</td></tr><tr><td>common-name</td><td>Common name of the user.</td></tr></table>	Option	Description	email	E-mail address of the user.	given-name	Given name of the user.	name	Unique name of the user.	upn	User principal name (UPN) of the user.	common-name	Common name of the user.			
Option	Description															
email	E-mail address of the user.															
given-name	Given name of the user.															
name	Unique name of the user.															
upn	User principal name (UPN) of the user.															
common-name	Common name of the user.															

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email-adfs-1x</i></td><td>E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.</td></tr><tr><td><i>group</i></td><td>Group that the user is a member of.</td></tr><tr><td><i>upn-adfs-1x</i></td><td>User principal name (UPN) of the user.</td></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>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>.			
	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>.																																			
group-claim-type	Group claim in assertion statement.	option	-	group																																
	<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																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email-adfs-1x</i></td><td>E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.</td></tr><tr><td><i>group</i></td><td>Group that the user is a member of.</td></tr><tr><td><i>upn-adfs-1x</i></td><td>User principal name (UPN) of the user.</td></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>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>.			
	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>.																																			
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.																																			

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 srcaddr <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set service <name1>, <name2>, ...
      next
    end
  next
end

```

config user security-exempt-list

Parameter	Description	Type	Size	Default
name	Name of the exempt list.	string	Maximum length: 35	
description	Description.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79	
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79	
service <name>	Destination services. Service name.	string	Maximum length: 79	

config user setting

Configure user authentication setting.

```

config user setting
    Description: Configure user authentication setting.
    set auth-type {option1}, {option2}, ...
    set auth-cert {string}
    set auth-ca-cert {string}
    set auth-secure-http [enable|disable]
    set auth-http-basic [enable|disable]
    set auth-ssl-allow-renegotiation [enable|disable]
    set auth-src-mac [enable|disable]
    set auth-on-demand [always|implicitly]
    set auth-portal-timeout {integer}
    set radius-ses-timeout-act [hard-timeout|ignore-timeout]
    set auth-blackout-time {integer}
    set auth-invalid-max {integer}
    set auth-lockout-threshold {integer}
    set auth-lockout-duration {integer}
    set per-policy-disclaimer [enable|disable]
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
        TELNET.
        edit <id>
            set type [http|https|...]
            set port {integer}
        next
    end
    set auth-ssl-min-proto-version [default|SSLv3|...]
    set auth-ssl-max-proto-version [ssl3|tlsv1|...]
    set auth-ssl-sigalgs [no-rsa-pss|all]
    set default-user-password-policy {string}
end

```

config user setting

Parameter	Description	Type	Size	Default										
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Allow HTTP authentication.</td></tr><tr><td><i>https</i></td><td>Allow HTTPS authentication.</td></tr><tr><td><i>ftp</i></td><td>Allow FTP authentication.</td></tr><tr><td><i>telnet</i></td><td>Allow TELNET authentication.</td></tr></table>				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.
	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.												
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35											

Parameter	Description	Type	Size	Default						
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35							
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-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-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-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-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: 1 Maximum value: 30	3						

Parameter	Description	Type	Size	Default						
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hard-timeout</i></td><td>Use session timeout from RADIUS as hard-timeout.</td></tr><tr><td><i>ignore-timeout</i></td><td>Ignore session timeout from RADIUS.</td></tr></table>	Option	Description	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.			
	Option	Description								
	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.								
<i>ignore-timeout</i>	Ignore session timeout from RADIUS.									
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 Maximum value: 3600	0						
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100	5						
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10	3						
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295	0						
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per policy disclaimer.</td></tr><tr><td><i>disable</i></td><td>Disable per policy disclaimer.</td></tr></table>	Option	Description	<i>enable</i>	Enable per policy disclaimer.	<i>disable</i>	Disable per policy disclaimer.			
	Option	Description								
	<i>enable</i>	Enable per policy disclaimer.								
<i>disable</i>	Disable per policy disclaimer.									
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></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.			
	Option	Description								
	<i>default</i>	Follow system global setting.								
<i>SSLv3</i>	SSLv3.									

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></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>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.					
	Option	Description														
	<i>TLSv1</i>	TLSv1.														
	<i>TLSv1-1</i>	TLSv1.1.														
	<i>TLSv1-2</i>	TLSv1.2.														
	<i>TLSv1-3</i>	TLSv1.3.														
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>ssl/v3</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>ssl/v3</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>ssl/v3</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-sigalgs	Set signature algorithms related to HTTPS authentication (affects TLS version <= 1.2 only, default is to enable all).	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 HTTPS authentication.</td></tr><tr><td><i>all</i></td><td>Enable all supported signature algorithms for HTTPS authentication.</td></tr></table>	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.									
	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.															
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													

config auth-ports

Parameter	Description	Type	Size	Default										
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
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><tr><td>ftp</td><td>FTP service.</td></tr><tr><td>telnet</td><td>TELNET service.</td></tr></table>				Option	Description	http	HTTP service.	https	HTTPS service.	ftp	FTP service.	telnet	TELNET service.
	Option	Description												
	http	HTTP service.												
	https	HTTPS service.												
	ftp	FTP service.												
telnet	TELNET service.													
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024										

config user tacacs+

Configure TACACS+ server entries.

```
config user tacacs+
  Description: Configure TACACS+ server entries.
  edit <name>
    set server {string}
    set secondary-server {string}
    set tertiary-server {string}
    set port {integer}
    set key {password}
    set secondary-key {password}
    set tertiary-key {password}
    set status-ttl {integer}
    set authen-type [mschap|chap|...]
    set authorization [enable|disable]
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
  next
end
```

config user tacacs+

Parameter	Description	Type	Size	Default												
name	TACACS+ server entry name.	string	Maximum length: 35													
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535	49												
key	Key to access the primary server.	password	Not Specified													
secondary-key	Key to access the secondary server.	password	Not Specified													
tertiary-key	Key to access the tertiary server.	password	Not Specified													
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												
authen-type	Allowed authentication protocols/methods.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mschap</i></td><td>MSCHAP.</td></tr><tr><td><i>chap</i></td><td>CHAP.</td></tr><tr><td><i>pap</i></td><td>PAP.</td></tr><tr><td><i>ascii</i></td><td>ASCII.</td></tr><tr><td><i>auto</i></td><td>Use PAP, MSCHAP, and CHAP (in that order).</td></tr></table>				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).
	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).															
authorization	Enable/disable TACACS+ authorization.	option	-	disable												

Parameter	Description	Type	Size	Default						
	<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.									
source-ip	Source IP address for communications to TACACS+ server.	string	Maximum length: 63							
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

videofilter

This section includes syntax for the following commands:

- [config videofilter keyword on page 1257](#)
- [config videofilter profile on page 1258](#)
- [config videofilter youtube-key on page 1261](#)

config videofilter keyword

Configure video filter keywords.

```
config videofilter keyword
  Description: Configure video filter keywords.
  edit <id>
    set name {string}
    set comment {var-string}
    set match [or|and]
    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
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
match	Keyword matching logic.	option	-	or
	Option	Description		
	<i>or</i>	Match any keyword.		
	<i>and</i>	Match all keywords.		

config word

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
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}
    config filters
      Description: YouTube filter entries.
      edit <id>
        set comment {var-string}
        set type [category|channel|...]
        set keyword {integer}

```

```

        set category {string}
        set channel {string}
        set action [allow|monitor|...]
        set log [enable|disable]
    next
end
set youtube [enable|disable]
set vimeo [enable|disable]
set dailymotion [enable|disable]
set replacemsg-group {string}
next
end

```

config videofilter profile

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 35							
comment	Comment.	var-string	Maximum length: 255							
youtube	Enable/disable YouTube video source.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable YouTube source.</td></tr><tr><td><i>disable</i></td><td>Disable YouTube source.</td></tr></table>	Option	Description	<i>enable</i>	Enable YouTube source.	<i>disable</i>	Disable YouTube source.			
Option	Description									
<i>enable</i>	Enable YouTube source.									
<i>disable</i>	Disable YouTube source.									
vimeo	Enable/disable Vimeo video source.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Vimeo source.</td></tr><tr><td><i>disable</i></td><td>Disable Vimeo source.</td></tr></table>	Option	Description	<i>enable</i>	Enable Vimeo source.	<i>disable</i>	Disable Vimeo source.			
Option	Description									
<i>enable</i>	Enable Vimeo source.									
<i>disable</i>	Disable Vimeo source.									
dailymotion	Enable/disable Dailymotion video source.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Dailymotion source.</td></tr><tr><td><i>disable</i></td><td>Disable Dailymotion source.</td></tr></table>	Option	Description	<i>enable</i>	Enable Dailymotion source.	<i>disable</i>	Disable Dailymotion source.			
Option	Description									
<i>enable</i>	Enable Dailymotion source.									
<i>disable</i>	Disable Dailymotion source.									
replacemsg-group	Replacement message group.	string	Maximum length: 35							

config filters

Parameter	Description	Type	Size	Default										
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
comment	Comment.	var-string	Maximum length: 255											
type	Filter type.	option	-	category										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>category</td><td>Filter videos by FortiGuard category.</td></tr><tr><td>channel</td><td>Filter videos by channel ID.</td></tr><tr><td>title</td><td>Filter videos by title.</td></tr><tr><td>description</td><td>Filter videos by description.</td></tr></table>				Option	Description	category	Filter videos by FortiGuard category.	channel	Filter videos by channel ID.	title	Filter videos by title.	description	Filter videos by description.
Option	Description													
category	Filter videos by FortiGuard category.													
channel	Filter videos by channel ID.													
title	Filter videos by title.													
description	Filter videos by description.													
keyword	Video filter keyword ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
category	FortiGuard category ID.	string	Maximum length: 7											
channel	Channel ID.	string	Maximum length: 255											
action	Video filter action.	option	-	monitor										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow videos to be accessed.</td></tr><tr><td>monitor</td><td>Monitor videos.</td></tr><tr><td>block</td><td>Block videos.</td></tr></table>				Option	Description	allow	Allow videos to be accessed.	monitor	Monitor videos.	block	Block videos.		
Option	Description													
allow	Allow videos to be accessed.													
monitor	Monitor videos.													
block	Block videos.													
log	Enable/disable logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging.</td></tr><tr><td>disable</td><td>Disable logging.</td></tr></table>				Option	Description	enable	Enable logging.	disable	Disable logging.				
Option	Description													
enable	Enable logging.													
disable	Disable logging.													

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 1262](#)

config virtual-patch profile

Configure virtual-patch profile.

```
config virtual-patch profile
  Description: Configure virtual-patch profile.
  edit <name>
    set comment {var-string}
    set severity {option1}, {option2}, ...
    set action [pass|block]
    set log [enable|disable]
    config exemption
      Description: Exempt devices or rules.
      edit <id>
        set status [enable|disable]
        set rule <id1>, <id2>, ...
        set device <mac1>, <mac2>, ...
      next
    end
  next
end
```

config virtual-patch profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
severity	Relative severity of the signature (low, medium, high, critical).	option	-	low medium high critical

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>low</i>	low		
	<i>medium</i>	medium		
	<i>high</i>	high		
	<i>critical</i>	critical		
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.		
log	Enable/disable logging of detection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		

config exemption

Parameter	Description	Type	Size	Default
id	IDs.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable exemption.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable exemption.		
	<i>disable</i>	Disable exemption.		
rule <id>	Patch signature rule IDs. Rule IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
device <mac>	Device MAC addresses. Device MAC address.	mac-address	Not Specified	

vpn

This section includes syntax for the following commands:

- [config vpn certificate ca on page 1264](#)
- [config vpn certificate crl on page 1266](#)
- [config vpn certificate hsm-local on page 1268](#)
- [config vpn certificate local on page 1272](#)
- [config vpn certificate ocsf-server on page 1277](#)
- [config vpn certificate remote on page 1278](#)
- [config vpn certificate setting on page 1279](#)
- [config vpn ipsec phase1-interface on page 1285](#)
- [config vpn ipsec phase2-interface on page 1304](#)
- [config vpn qkd on page 1312](#)

config vpn certificate ca

CA certificate.

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

config vpn certificate ca

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 79									
ca	CA certificate as a PEM file.	user	Not Specified									
range	Either global or VDOM IP address range for the CA 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	CA 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.											
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Trusted CA for SSL inspection.</td></tr><tr><td>disable</td><td>Untrusted CA for SSL inspection.</td></tr></table>				Option	Description	enable	Trusted CA for SSL inspection.	disable	Untrusted CA for SSL inspection.		
Option	Description											
enable	Trusted CA for SSL inspection.											
disable	Untrusted CA for SSL inspection.											
scep-url	URL of the SCEP server.	string	Maximum length: 255									
est-url	URL of the EST server.	string	Maximum length: 255									
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								

Parameter	Description	Type	Size	Default						
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0						
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255							
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.									
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.									

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 range [global|vdom]
    set source [factory|user|...]
    set update-vdom {string}
    set ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set http-url {string}
    set scep-url {string}
    set scep-cert {string}
    set update-interval {integer}
    set source-ip {ipv4-address}
  next
end

```

config vpn certificate crl

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
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.											
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.											
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									
ldap-password	LDAP server user password.	password	Not Specified									
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255									
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								
update-interval	Time in seconds before the FortiProxy checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0								
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0								

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

config vpn certificate hsm-local

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comments	Comment.	string	Maximum length: 511	
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.											
api-version	API version for communicating with HSM.	option	-	unknown								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unknown</i></td><td>Unknown API version.</td></tr><tr><td><i>gch-default</i></td><td>Google Cloud HSM default API.</td></tr></table>	Option	Description	<i>unknown</i>	Unknown API version.	<i>gch-default</i>	Google Cloud HSM default API.					
	Option	Description										
	<i>unknown</i>	Unknown API version.										
<i>gch-default</i>	Google Cloud HSM default API.											
certificate	PEM format certificate.	user		Not Specified								
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.											
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
gch-url	Google Cloud HSM key URL (e.g. "https://cloudkms.googleapis.com/v1/projects/sampleproject/locations/samplelocation/keyRings/samplekeyring/cryptoKeys/sampleKeyName/cryptoKeyVersions/1").	string	Maximum length: 1024	
gch-project	Google Cloud HSM project ID.	string	Maximum length: 31	
gch-location	Google Cloud HSM location.	string	Maximum length: 63	
gch-keyring	Google Cloud HSM keyring.	string	Maximum length: 63	
gch-cryptokey	Google Cloud HSM cryptokey.	string	Maximum length: 63	
gch-cryptokey-version	Google Cloud HSM cryptokey version.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
gch-cloud-service-name	Cloud service config name to generate access token.	string	Maximum length: 35	
gch-cryptkey-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.
<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.

Parameter	Description	Type	Size	Default
Option	Description			
<i>ec-sign-p384-sha384</i>	Elliptic Curve P-384 - SHA384 Digest.			
<i>ec-sign-secp256k1-sha256</i>	Elliptic Curve secp256k1 - SHA256 Digest.			

config vpn certificate local

Local keys and certificates.

```

config vpn certificate local
  Description: Local keys and certificates.
  edit <name>
    set type [normal|hsm]
    set password {password}
    set hsm-vendor [safenet|primus]
    set hsm-slot {string}
    set hsm-keytype [rsa|ec]
    set comments {string}
    set private-key {user}
    set certificate {user}
    set csr {user}
    set state {user}
    set scep-url {string}
    set range [global|vdom]
    set source [factory|user|...]
    set auto-regenerate-days {integer}
    set auto-regenerate-days-warning {integer}
    set scep-password {password}
    set ca-identifier {string}
    set name-encoding [printable|utf8]
    set source-ip {ipv4-address}
    set ike-localid {string}
    set ike-localid-type [asn1dn|fqdn]
    set enroll-protocol [none|scep|...]
    set private-key-retain [enable|disable]
    set cmp-server {string}
    set cmp-path {string}
    set cmp-server-cert {string}
    set cmp-regeneration-method [keyupdate|renewal]
    set acme-ca-url {string}
    set acme-domain {string}
    set acme-email {string}

```

```

set acme-rsa-key-size {integer}
set acme-renew-window {integer}
set est-server {string}
set est-ca-id {string}
set est-http-username {string}
set est-http-password {string}
set est-client-cert {string}
set est-server-cert {string}
set est-srp-username {string}
set est-srp-password {string}
set est-regeneration-method [create-new-key|use-existing-key]
next
end

```

config vpn certificate local

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Type.	option	-	normal
	Option	Description		
	normal	Normal		
	hsm	HSM		
password	Password as a PEM file.	password	Not Specified	
hsm-vendor	HSM vendor.	option	-	safenet
	Option	Description		
	safenet	Safenet HSM.		
	primus	Securosys Primus HSM.		
hsm-slot	HSM slot to use with this certificate.	string	Maximum length: 35	
hsm-keytype	HSM certificate key type.	option	-	rsa
	Option	Description		
	rsa	RSA key type.		
	ec	EC key type.		
comments	Comment.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default								
private-key	PEM format key encrypted with a password.	user	Not Specified									
certificate	PEM format certificate.	user	Not Specified									
csr	Certificate Signing Request.	user	Not Specified									
state	Certificate Signing Request State.	user	Not Specified									
scep-url	SCEP server URL.	string	Maximum length: 255									
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.											
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								

Parameter	Description	Type	Size	Default												
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified													
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255													
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.															
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0												
ike-localid	Local ID the FortiProxy 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><i>asn1dn</i></td><td>ASN.1 distinguished name.</td></tr><tr><td><i>fqdn</i></td><td>Fully qualified domain name.</td></tr></table>				Option	Description	<i>asn1dn</i>	ASN.1 distinguished name.	<i>fqdn</i>	Fully qualified domain name.						
Option	Description															
<i>asn1dn</i>	ASN.1 distinguished name.															
<i>fqdn</i>	Fully qualified domain name.															
enroll-protocol	Certificate enrollment protocol.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None (default).</td></tr><tr><td><i>scep</i></td><td>Simple Certificate Enrollment Protocol.</td></tr><tr><td><i>cmpv2</i></td><td>Certificate Management Protocol Version 2.</td></tr><tr><td><i>acme2</i></td><td>Automated Certificate Management Environment Version 2.</td></tr><tr><td><i>est</i></td><td>Enrollment over Secure Transport.</td></tr></table>				Option	Description	<i>none</i>	None (default).	<i>scep</i>	Simple Certificate Enrollment Protocol.	<i>cmpv2</i>	Certificate Management Protocol Version 2.	<i>acme2</i>	Automated Certificate Management Environment Version 2.	<i>est</i>	Enrollment over Secure Transport.
Option	Description															
<i>none</i>	None (default).															
<i>scep</i>	Simple Certificate Enrollment Protocol.															
<i>cmpv2</i>	Certificate Management Protocol Version 2.															
<i>acme2</i>	Automated Certificate Management Environment Version 2.															
<i>est</i>	Enrollment over Secure Transport.															
private-key-retain	Enable/disable retention of private key during SCEP renewal (default = disable).	option	-	disable												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Keep the existing private key during SCEP renewal.		
	<i>disable</i>	Generate a new private key during SCEP renewal.		
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63	
cmp-path	Path location inside CMP server.	string	Maximum length: 255	
cmp-server-cert	CMP server certificate.	string	Maximum length: 79	
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate
	Option	Description		
	<i>keyupate</i>	Key Update.		
	<i>renewal</i>	Renewal.		
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 FortiProxy unit.	string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
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
acme-renew-window	Beginning of the renewal window (in days before certificate expiration, 30 by default).	integer	Minimum value: 1 Maximum value: 100	30
est-server	Address and port for EST server (e.g. https://example.com:1234).	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
est-ca-id	CA identifier of the CA server for signing via EST.	string	Maximum length: 255							
est-http-username	HTTP Authentication username for signing via EST.	string	Maximum length: 63							
est-http-password	HTTP Authentication password for signing via EST.	string	Maximum length: 63							
est-client-cert	Certificate used to authenticate this FortiGate to EST server.	string	Maximum length: 79							
est-server-cert	EST server's certificate must be verifiable by this certificate to be authenticated.	string	Maximum length: 79							
est-srp-username	EST SRP authentication username.	string	Maximum length: 63							
est-srp-password	EST SRP authentication password.	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><i>create-new-key</i></td><td>Create new private key during re-enrollment.</td></tr><tr><td><i>use-existing-key</i></td><td>Reuse existing private key during re-enrollment.</td></tr></table>				Option	Description	<i>create-new-key</i>	Create new private key during re-enrollment.	<i>use-existing-key</i>	Reuse existing private key during re-enrollment.
Option	Description									
<i>create-new-key</i>	Create new private key during re-enrollment.									
<i>use-existing-key</i>	Reuse existing private key during re-enrollment.									

config vpn certificate ocsf-server

OCSP server configuration.

```

config vpn certificate ocsf-server
  Description: OCSP server configuration.
  edit <name>
    set url {string}
    set cert {string}
    set secondary-url {string}
    set secondary-cert {string}

```

```

        set unavail-action [revoke|ignore]
        set source-ip {string}
    next
end

```

config vpn certificate ocsf-server

Parameter	Description	Type	Size	Default						
name	OCSP server entry name.	string	Maximum length: 35							
url	OCSP server URL.	string	Maximum length: 127							
cert	OCSP server certificate.	string	Maximum length: 127							
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127							
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127							
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-	revoke						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>revoke</td><td>Revoke certificate if server is unavailable.</td></tr><tr><td>ignore</td><td>Ignore OCSP check if server is unavailable.</td></tr></table>				Option	Description	revoke	Revoke certificate if server is unavailable.	ignore	Ignore OCSP check if server is unavailable.
	Option	Description								
	revoke	Revoke certificate if server is unavailable.								
ignore	Ignore OCSP check if server is unavailable.									
source-ip	Source IP address for dynamic AIA and OCSP queries.	string	Maximum length: 63							

config vpn certificate remote

Remote certificate as a PEM file.

```

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

```

config vpn certificate remote

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
remote	Remote certificate.	user	Not Specified									
range	Either the global or VDOM IP address range for the remote 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.											
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.											

config vpn certificate setting

VPN certificate setting.

```
config vpn certificate setting
  Description: VPN certificate setting.
  set ocsdp-status [enable|mandatory|...]
  set ocsdp-option [certificate|server]
  set proxy {string}
  set proxy-port {integer}
  set proxy-username {string}
  set proxy-password {password}
  set source-ip {string}
  set ocsdp-default-server {string}
  set interface-select-method [auto|specify]
  set interface {string}
  set check-ca-cert [enable|disable]
  set check-ca-chain [enable|disable]
  set subject-match [substring|value]
  set subject-set [subset|superset]
  set cn-match [substring|value]
  set cn-allow-multi [disable|enable]
```

```

config crl-verification
    Description: CRL verification options.
    set expiry [ignore|revoke]
    set leaf-crl-absence [ignore|revoke]
    set chain-crl-absence [ignore|revoke]
end
set strict-ocsp-check [enable|disable]
set ssl-min-proto-version [default|SSLv3|...]
set cmp-save-extra-certs [enable|disable]
set cmp-key-usage-checking [enable|disable]
set cert-expire-warning {integer}
set certname-rsa1024 {string}
set certname-rsa2048 {string}
set certname-rsa4096 {string}
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}
end

```

config vpn certificate setting

Parameter	Description	Type	Size	Default								
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>OCSP is performed if CRL is not checked.</td></tr><tr><td><i>mandatory</i></td><td>If cert is not revoked by CRL, OCSP is performed.</td></tr><tr><td><i>disable</i></td><td>OCSP is not performed.</td></tr></table>	Option	Description	<i>enable</i>	OCSP is performed if CRL is not checked.	<i>mandatory</i>	If cert is not revoked by CRL, OCSP is performed.	<i>disable</i>	OCSP is not performed.			
Option	Description											
<i>enable</i>	OCSP is performed if CRL is not checked.											
<i>mandatory</i>	If cert is not revoked by CRL, OCSP is performed.											
<i>disable</i>	OCSP is not performed.											
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><i>certificate</i></td><td>Use URL from certificate.</td></tr><tr><td><i>server</i></td><td>Use URL from configured OCSP server.</td></tr></table>	Option	Description	<i>certificate</i>	Use URL from certificate.	<i>server</i>	Use URL from configured OCSP server.					
Option	Description											
<i>certificate</i>	Use URL from certificate.											
<i>server</i>	Use URL from configured OCSP server.											
proxy	Proxy server FQDN or IP for OCSP/CA queries during certificate verification.	string	Maximum length: 127									

Parameter	Description	Type	Size	Default						
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							
proxy-password	Proxy server password.	password	Not Specified							
source-ip	Source IP address for dynamic AIA and OCSP queries.	string	Maximum length: 63							
ocsp-default-server	Default OCSP server.	string	Maximum length: 35							
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>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
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						

Parameter	Description	Type	Size	Default						
	<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.									
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><i>substring</i></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><i>value</i></td><td>Find a match if the name being searched for is same as a certificate subject RDN.</td></tr></table>	Option	Description	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate subject RDN.	<i>value</i>	Find a match if the name being searched for is same as a certificate subject RDN.			
	Option	Description								
	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate subject RDN.								
<i>value</i>	Find a match if the name being searched for is same as a certificate subject RDN.									
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.									
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><i>substring</i></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><i>value</i></td><td>Find a match if the name being searched for is same as a certificate CN.</td></tr></table>	Option	Description	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate CN.	<i>value</i>	Find a match if the name being searched for is same as a certificate CN.			
	Option	Description								
	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate CN.								
<i>value</i>	Find a match if the name being searched for is same as a certificate CN.									
cn-allow-multi	When searching for a matching certificate, allow multiple CN fields in certificate subject name (default = enable).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Does not allow multiple CN entries in certificate matching.		
	<i>enable</i>	Allow multiple CN entries in certificate matching.		
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable
	Option Description			
	<i>enable</i>	Enable strict mode OCSP checking.		
	<i>disable</i>	Disable strict mode OCSP checking.		
ssl-min-protocol-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.		
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode (default = disable).	option	-	disable
	Option Description			
	<i>enable</i>	Enable saving extra certificates in CMP mode.		
	<i>disable</i>	Disable saving extra certificates in CMP mode.		
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode (default = enable).	option	-	enable
	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.		

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-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
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

config crt-verification

Parameter	Description	Type	Size	Default
expiry	CRL verification option when CRL is expired (default = ignore).	option	-	ignore

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ignore</i></td><td>Certificate status will be verified even if CRL is expired.</td></tr><tr><td><i>revoke</i></td><td>Certificate will be revoked if CRL is expired.</td></tr></table>	Option	Description	<i>ignore</i>	Certificate status will be verified even if CRL is expired.	<i>revoke</i>	Certificate will be revoked if CRL is expired.			
Option	Description									
<i>ignore</i>	Certificate status will be verified even if CRL is expired.									
<i>revoke</i>	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><i>ignore</i></td><td>CRL verification against leaf certificate is ignored if CRL is absent.</td></tr><tr><td><i>revoke</i></td><td>Certificate will be revoked if CRL of leaf certificate is absent.</td></tr></table>	Option	Description	<i>ignore</i>	CRL verification against leaf certificate is ignored if CRL is absent.	<i>revoke</i>	Certificate will be revoked if CRL of leaf certificate is absent.			
Option	Description									
<i>ignore</i>	CRL verification against leaf certificate is ignored if CRL is absent.									
<i>revoke</i>	Certificate will be revoked if CRL of leaf certificate is absent.									
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><i>ignore</i></td><td>CRL verification is ignored if CRL of any certificate in chain is absent.</td></tr><tr><td><i>revoke</i></td><td>Certificate will be revoked if CRL of any certificate in chain is absent.</td></tr></table>	Option	Description	<i>ignore</i>	CRL verification is ignored if CRL of any certificate in chain is absent.	<i>revoke</i>	Certificate will be revoked if CRL of any certificate in chain is absent.			
Option	Description									
<i>ignore</i>	CRL verification is ignored if CRL of any certificate in chain is absent.									
<i>revoke</i>	Certificate will be revoked if CRL of any certificate in chain is absent.									

config vpn ipsec phase1-interface

Configure VPN remote gateway.

```

config vpn ipsec phase1-interface
  Description: Configure VPN remote gateway.
  edit <name>
    set interface {string}
    set ip-version {option}
    set ike-version [1|2]
    set local-gw {ipv4-address}
    set remote-gw {ipv4-address}
    set keylife {integer}
    set certificate <name1>, <name2>, ...
    set authmethod [psk|signature]
    set mode [aggressive|main]
    set peertype {option}
    set peerid {string}
    set peer {string}
    set aggregate-member {option}
    set packet-redistribution [enable|disable]
    set proposal {option1}, {option2}, ...
    set psksecret {password-3}
  
```

```
set keepalive {integer}
set distance {integer}
set priority {integer}
set localid {string}
set localid-type [auto|fqdn|...]
set negotiate-timeout {integer}
set fragmentation [enable|disable]
set comments {var-string}
set send-cert-chain [enable|disable]
set dhgrp {option1}, {option2}, ...
set eap [enable|disable]
set eap-identity [use-id-payload|send-request]
set eap-exclude-peergrp {string}
set eap-cert-auth [enable|disable]
set acct-verify [enable|disable]
set ppk [disable|allow|...]
set ppk-secret {password-3}
set ppk-identity {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
set reauth [disable|enable]
set authusr {string}
set authpasswd {password}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set authusrgrp {string}
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set fgsp-sync [enable|disable]
set inbound-dscp-copy [enable|disable]
set auto-discovery-sender [enable|disable]
set auto-discovery-receiver [enable|disable]
set auto-discovery-forwarder [enable|disable]
set auto-discovery-psk [enable|disable]
set auto-discovery-shortcuts [independent|dependent]
set auto-discovery-crossover [allow|block]
set auto-discovery-offer-interval {integer}
set fragmentation-mtu {integer}
set childless-ike [enable|disable]
set azure-ad-autoconnect [enable|disable]
set client-resume [enable|disable]
set client-resume-interval {integer}
set rekey [enable|disable]
set digital-signature-auth [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set rsa-signature-format [pkcs1|pss]
set rsa-signature-hash-override [enable|disable]
set enforce-unique-id [disable|keep-new|...]
set cert-id-validation [enable|disable]
set network-overlay [disable|enable]
set network-id {integer}
set dev-id-notification [disable|enable]
```

```

set dev-id {string}
set loopback-asymroute [enable|disable]
set link-cost {integer}
set kms {string}
set exchange-fgt-device-id [enable|disable]
set ems-sn-check [enable|disable]
set cert-trust-store [local|ems]
set qkd [disable|allow|...]
set qkd-profile {string}
set transport [udp|udp-fallback-tcp|...]
set fortinet-esp [enable|disable]
set remote-gw-match [any|ipmask|...]
set remote-gw-subnet {ipv4-classnet-any}
set remote-gw-start-ip {ipv4-address-any}
set remote-gw-end-ip {ipv4-address-any}
set remote-gw-country {string}
set remote-gw6-match [any|ipprefix|...]
set remote-gw6-subnet {ipv6-network}
set remote-gw6-start-ip {ipv6-address}
set remote-gw6-end-ip {ipv6-address}
set remote-gw6-country {string}
set cert-peer-username-validation [none|othername|...]
set cert-peer-username-strip [disable|enable]
next
end

```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default						
name	IPsec remote gateway name.	string	Maximum length: 15							
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35							
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></table>				Option	Description	4	Use IPv4 addressing for gateways.		
Option	Description									
4	Use IPv4 addressing for gateways.									
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.									

Parameter	Description	Type	Size	Default						
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400						
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79							
authmethod	Authentication method.	option	-	psk						
	<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.									
mode	The ID protection mode used to establish a secure channel.	option	-	main						
	<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.									
peertype	Accept this peer type.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer ID.</td></tr></table>				Option	Description	<i>any</i>	Accept any peer ID.		
Option	Description									
<i>any</i>	Accept any peer ID.									
peerid	Accept this peer identity.	string	Maximum length: 255							
peer	Accept this peer certificate.	string	Maximum length: 35							
aggregate-member	Enable/disable use as an aggregate member.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use as an aggregate member.</td></tr></table>				Option	Description	<i>disable</i>	Disable use as an aggregate member.		
Option	Description									
<i>disable</i>	Disable use as an aggregate member.									

Parameter	Description	Type	Size	Default																																										
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.																																													
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><tr><td><i>aes128-md5</i></td><td>aes128-md5</td></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>aes128gcm-prfsha1</i></td><td>aes128gcm-prfsha1</td></tr><tr><td><i>aes128gcm-prfsha256</i></td><td>aes128gcm-prfsha256</td></tr><tr><td><i>aes128gcm-prfsha384</i></td><td>aes128gcm-prfsha384</td></tr><tr><td><i>aes128gcm-prfsha512</i></td><td>aes128gcm-prfsha512</td></tr><tr><td><i>aes192-md5</i></td><td>aes192-md5</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	<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			
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																																													

Parameter	Description	Type	Size	Default
	Option	Description		
	<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		
	<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		

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></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>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>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																													
keepalive	NAT-T keep alive interval.	integer	Minimum value: 5 Maximum value: 900	10																												
distance	Distance for routes added by IKE (1 - 255).	integer	Minimum value: 1 Maximum value: 255	15																												
priority	Priority for routes added by IKE (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535	1																												
localid	Local ID.	string	Maximum length: 63																													
localid-type	Local ID type.	option	-	auto																												

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Select ID type automatically.</td></tr><tr><td><i>fqdn</i></td><td>Use fully qualified domain name.</td></tr><tr><td><i>user-fqdn</i></td><td>Use user fully qualified domain name.</td></tr><tr><td><i>keyid</i></td><td>Use key-id string.</td></tr><tr><td><i>address</i></td><td>Use local IP address.</td></tr><tr><td><i>asn1dn</i></td><td>Use ASN.1 distinguished name.</td></tr></table>	Option	Description	<i>auto</i>	Select ID type automatically.	<i>fqdn</i>	Use fully qualified domain name.	<i>user-fqdn</i>	Use user fully qualified domain name.	<i>keyid</i>	Use key-id string.	<i>address</i>	Use local IP address.	<i>asn1dn</i>	Use ASN.1 distinguished name.			
	Option	Description																
	<i>auto</i>	Select ID type automatically.																
	<i>fqdn</i>	Use fully qualified domain name.																
	<i>user-fqdn</i>	Use user fully qualified domain name.																
	<i>keyid</i>	Use key-id string.																
	<i>address</i>	Use local IP address.																
<i>asn1dn</i>	Use ASN.1 distinguished name.																	
negotiate-timeout	IKE SA negotiation timeout in seconds (1 - 300).	integer	Minimum value: 1 Maximum value: 300	30														
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intra-IKE fragmentation support on re-transmission.</td></tr><tr><td><i>disable</i></td><td>Disable intra-IKE fragmentation support.</td></tr></table>	Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.											
	Option	Description																
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.																
<i>disable</i>	Disable intra-IKE fragmentation support.																	
comments	Comment.	var-string	Maximum length: 255															
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending certificate chain.</td></tr><tr><td><i>disable</i></td><td>Disable sending certificate chain.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending certificate chain.	<i>disable</i>	Disable sending certificate chain.											
	Option	Description																
	<i>enable</i>	Enable sending certificate chain.																
<i>disable</i>	Disable sending certificate chain.																	
dhgrp	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></table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.					
	Option	Description																
	1	DH Group 1.																
	2	DH Group 2.																
	5	DH Group 5.																
	14	DH Group 14.																
15	DH Group 15.																	

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></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	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																												
	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.																												
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.																													
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>use-id-payload</td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td>send-request</td><td>Use EAP identity request to resolve peer identity.</td></tr></table>	Option	Description	use-id-payload	Use IKEv2 IDi payload to resolve peer identity.	send-request	Use EAP identity request to resolve peer identity.																							
	Option	Description																												
	use-id-payload	Use IKEv2 IDi payload to resolve peer identity.																												
send-request	Use EAP identity request to resolve peer identity.																													
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35																											
eap-cert-auth	Enable/disable peer certificate authentication in addition to EAP if peer is a FortiClient endpoint.	option	-	disable																										

Parameter	Description	Type	Size	Default
	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.		
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.		
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable
	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-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	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.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dialup-windows</i></td><td>Dial Up - Windows Native IPsec Client.</td></tr><tr><td><i>dialup-cisco</i></td><td>Dial Up - Cisco IPsec Client.</td></tr><tr><td><i>static-fortiproxy</i></td><td>Site to Site - FortiProxy.</td></tr><tr><td><i>dialup-fortiproxy</i></td><td>Dial Up - FortiProxy.</td></tr><tr><td><i>static-cisco</i></td><td>Site to Site - Cisco.</td></tr><tr><td><i>dialup-cisco-fw</i></td><td>Dialup Up - Cisco Firewall.</td></tr><tr><td><i>simplified-static-fortiproxy</i></td><td>Site to Site - FortiProxy (SD-WAN).</td></tr><tr><td><i>hub-fortiproxy-auto-discovery</i></td><td>Hub role in a Hub-and-Spoke auto-discovery VPN.</td></tr><tr><td><i>spoke-fortiproxy-auto-discovery</i></td><td>Spoke role in a Hub-and-Spoke auto-discovery VPN.</td></tr></table>	Option	Description	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	<i>static-fortiproxy</i>	Site to Site - FortiProxy.	<i>dialup-fortiproxy</i>	Dial Up - FortiProxy.	<i>static-cisco</i>	Site to Site - Cisco.	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	<i>simplified-static-fortiproxy</i>	Site to Site - FortiProxy (SD-WAN).	<i>hub-fortiproxy-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.	<i>spoke-fortiproxy-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.			
	Option	Description																						
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.																						
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.																						
	<i>static-fortiproxy</i>	Site to Site - FortiProxy.																						
	<i>dialup-fortiproxy</i>	Dial Up - FortiProxy.																						
	<i>static-cisco</i>	Site to Site - Cisco.																						
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.																						
	<i>simplified-static-fortiproxy</i>	Site to Site - FortiProxy (SD-WAN).																						
<i>hub-fortiproxy-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.																							
<i>spoke-fortiproxy-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.																							
xauthtype	XAuth type.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>client</i></td><td>Enable as client.</td></tr><tr><td><i>pap</i></td><td>Enable as server PAP.</td></tr><tr><td><i>chap</i></td><td>Enable as server CHAP.</td></tr><tr><td><i>auto</i></td><td>Enable as server auto.</td></tr></table>	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.											
	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.																							
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.																							

Parameter	Description	Type	Size	Default						
authusr	XAuth user name.	string	Maximum length: 64							
authpasswd	XAuth password (max 35 characters).	password	Not Specified							
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 IDi group authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 IDi group authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable IKEv2 IDi group authentication.	<i>disable</i>	Disable IKEv2 IDi group authentication.
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							
authusrgrp	Authentication user group.	string	Maximum length: 35							
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable						
	<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: 5 Maximum value: 43200	15						
fgsp-sync	Enable/disable IPsec syncing of tunnels for FGSP IPsec.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec syncing of tunnels to other cluster members.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec syncing of tunnels to other cluster members.</td></tr></table>				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.
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.									
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable						

Parameter	Description	Type	Size	Default
	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.		
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sending auto-discovery short-cut messages.		
	<i>disable</i>	Disable sending auto-discovery short-cut messages.		
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable receiving auto-discovery short-cut messages.		
	<i>disable</i>	Disable receiving auto-discovery short-cut messages.		
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.		
	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.		
auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-	disable
	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-shortcuts	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent

Parameter	Description	Type	Size	Default
	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-discovery-crossover	Allow/block set-up of short-cut tunnels between different network IDs.	option	-	allow
	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-offer-interval	Interval between shortcut offer messages in seconds (1 - 300, default = 5).	integer	Minimum value: 1 Maximum value: 300	5
fragmentation-mtu	IKE fragmentation MTU (500 - 16000).	integer	Minimum value: 500 Maximum value: 16000	1200
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).		
azure-ad-autoconnect	Enable/disable Azure AD Auto-Connect for FortiClient.	option	-	disable
	Option Description			
	<i>enable</i>	Enable Azure AD Auto-Connect for FortiClient.		
	<i>disable</i>	Disable Azure AD Auto-Connect for FortiClient.		

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><i>enable</i></td><td>Enable client session resumption.</td></tr><tr><td><i>disable</i></td><td>Disable client session resumption.</td></tr></table>	Option	Description	<i>enable</i>	Enable client session resumption.	<i>disable</i>	Disable client session resumption.			
Option	Description									
<i>enable</i>	Enable client session resumption.									
<i>disable</i>	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						
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.									
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).	<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).			
Option	Description									
<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).									
<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).									
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha1</i></td><td>SHA1.</td></tr></table>	Option	Description	<i>sha1</i>	SHA1.					
Option	Description									
<i>sha1</i>	SHA1.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha2-256</i></td><td>SHA2-256.</td></tr><tr><td><i>sha2-384</i></td><td>SHA2-384.</td></tr><tr><td><i>sha2-512</i></td><td>SHA2-512.</td></tr></table>	Option	Description	<i>sha2-256</i>	SHA2-256.	<i>sha2-384</i>	SHA2-384.	<i>sha2-512</i>	SHA2-512.			
	Option	Description										
	<i>sha2-256</i>	SHA2-256.										
	<i>sha2-384</i>	SHA2-384.										
<i>sha2-512</i>	SHA2-512.											
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pkcs1</i></td><td>RSASSA PKCS#1 v1.5.</td></tr><tr><td><i>pss</i></td><td>RSASSA Probabilistic Signature Scheme (PSS).</td></tr></table>	Option	Description	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).					
	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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 RSA signature hash algorithm override.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 RSA signature hash algorithm override.</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 RSA signature hash algorithm override.	<i>disable</i>	Disable IKEv2 RSA signature hash algorithm override.					
	Option	Description										
	<i>enable</i>	Enable IKEv2 RSA signature hash algorithm override.										
<i>disable</i>	Disable IKEv2 RSA signature hash algorithm override.											
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.											
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><i>enable</i></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><i>disable</i></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	<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.					
	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.											

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.									
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0						
dev-id-notification	Enable/disable device ID notification.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable device ID notification.</td></tr><tr><td><i>enable</i></td><td>Enable device ID notification.</td></tr></table>	Option	Description	<i>disable</i>	Disable device ID notification.	<i>enable</i>	Enable device ID notification.			
Option	Description									
<i>disable</i>	Disable device ID notification.									
<i>enable</i>	Enable device ID notification.									
dev-id	Device ID carried by the device ID notification.	string	Maximum length: 63							
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow ingress/egress IKE traffic to be routed over different interfaces.</td></tr><tr><td><i>disable</i></td><td>Ingress/egress IKE traffic must be routed over the same interface.</td></tr></table>	Option	Description	<i>enable</i>	Allow ingress/egress IKE traffic to be routed over different interfaces.	<i>disable</i>	Ingress/egress IKE traffic must be routed over the same interface.			
Option	Description									
<i>enable</i>	Allow ingress/egress IKE traffic to be routed over different interfaces.									
<i>disable</i>	Ingress/egress IKE traffic must be routed over the same interface.									
link-cost	VPN tunnel underlay link cost.	integer	Minimum value: 0 Maximum value: 255	0						
kms	Key Management Services server.	string	Maximum length: 35							
exchange-fgt-device-id	Enable/disable device identifier exchange with peer FortiGate units for use of VPN monitor data by FortiManager.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable exchange of FortiGate device identifier.		
	<i>disable</i>	Disable exchange of FortiGate device identifier.		
ems-sn-check	Enable/disable verification of EMS serial number.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable EMS serial number verification.		
	<i>disable</i>	Disable EMS serial number verification.		
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.		
qkd	Enable/disable use of Quantum Key Distribution (QKD) server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of a Quantum Key Distribution (QKD) server.		
	<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-profile	Quantum Key Distribution (QKD) server profile.	string	Maximum length: 35	
transport	Set IKE transport protocol.	option	-	udp
	Option	Description		
	<i>udp</i>	Use UDP transport for IKE.		
	<i>udp-fallback-tcp</i>	Use UDP transport for IKE, with fallback to TCP transport.		
	<i>tcp</i>	Use TCP transport for IKE.		
fortinet-esp	Enable/disable Fortinet ESP encapsulation.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Fortinet ESP encapsulation.</td></tr><tr><td><i>disable</i></td><td>Disable Fortinet ESP encapsulaton.</td></tr></table>	Option	Description	<i>enable</i>	Enable Fortinet ESP encapsulation.	<i>disable</i>	Disable Fortinet ESP encapsulaton.							
	Option	Description												
	<i>enable</i>	Enable Fortinet ESP encapsulation.												
<i>disable</i>	Disable Fortinet ESP encapsulaton.													
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></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.			
	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.													
remote-gw-subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0										
remote-gw-start-ip	First IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0										
remote-gw-end-ip	Last IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0										
remote-gw-country	IPv4 addresses associated to a specific country.	string	Maximum length: 2											
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-subnet	IPv6 address and prefix.	ipv6-network	Not Specified	::/0										
remote-gw6-start-ip	First IPv6 address in the range.	ipv6-address	Not Specified	::										
remote-gw6-end-ip	Last IPv6 address in the range.	ipv6-address	Not Specified	::										

Parameter	Description	Type	Size	Default										
remote-gw6-country	IPv6 addresses associated to a specific country.	string	Maximum length: 2											
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><i>none</i></td><td>Disable cross validation of peer username and the identity in the peer's certificate.</td></tr><tr><td><i>othername</i></td><td>Validate principal name in SAN othername.</td></tr><tr><td><i>rfc822name</i></td><td>Validate RFC822 email address in SAN.</td></tr><tr><td><i>cn</i></td><td>Validate CN in subject.</td></tr></table>	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.			
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-peer-username-strip	Enable/disable domain stripping on certificate identity.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable domain stripping on certificate identity.</td></tr><tr><td><i>enable</i></td><td>Enable domain stripping on certificate identity.</td></tr></table>	Option	Description	<i>disable</i>	Disable domain stripping on certificate identity.	<i>enable</i>	Enable domain stripping on certificate identity.							
Option	Description													
<i>disable</i>	Disable domain stripping on certificate identity.													
<i>enable</i>	Enable domain stripping on certificate identity.													

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```

config vpn ipsec phase2-interface
  Description: Configure VPN autokey tunnel.
  edit <name>
    set phase1name {string}
    set proposal {option1}, {option2}, ...
    set dhgrp {option1}, {option2}, ...
    set replay [enable|disable]
    set keepalive [enable|disable]
    set auto-negotiate [enable|disable]
    set add-route [phase1|enable|...]
    set inbound-dscp-copy [phase1|enable|...]
    set auto-discovery-sender [phase1|enable|...]
    set auto-discovery-forwarder [phase1|enable|...]
    set keylifeseconds {integer}
    set keylifekbs {integer}
    set keylife-type [seconds|kbs|...]
    set single-source [enable|disable]
    set route-overlap [use-old|use-new|...]
    set comments {var-string}
  
```

```

set protocol {integer}
set src-name {string}
set src-name6 {string}
set src-addr-type [subnet|range|...]
set src-start-ip {ipv4-address-any}
set src-start-ip6 {ipv6-address}
set src-end-ip {ipv4-address-any}
set src-end-ip6 {ipv6-address}
set src-subnet {ipv4-classnet-any}
set src-subnet6 {ipv6-prefix}
set src-port {integer}
set dst-name {string}
set dst-name6 {string}
set dst-addr-type [subnet|range|...]
set dst-start-ip {ipv4-address-any}
set dst-start-ip6 {ipv6-address}
set dst-end-ip {ipv4-address-any}
set dst-end-ip6 {ipv6-address}
set dst-subnet {ipv4-classnet-any}
set dst-subnet6 {ipv6-prefix}
set dst-port {integer}
next
end

```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default																		
name	IPsec tunnel name.	string	Maximum length: 35																			
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15																			
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></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
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																					

Parameter	Description	Type	Size	Default

Option	Description
<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
<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

Parameter	Description	Type	Size	Default																																																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chacha20poly1305</i></td><td>chacha20poly1305</td></tr><tr><td><i>aria128-null</i></td><td>aria128-null</td></tr><tr><td><i>aria128-md5</i></td><td>aria128-md5</td></tr><tr><td><i>aria128-sha1</i></td><td>aria128-sha1</td></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-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>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	<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>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																																																							
	<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																																																							
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></table>		Option	Description	1	DH Group 1.																																																			
	Option	Description																																																							
1	DH Group 1.																																																								

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></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	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																																				
	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.																																				
replay	Enable/disable replay detection.	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.																																					
keepalive	Enable/disable keep alive.	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.																																					
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></table>	Option	Description	enable	Enable setting.																																	
	Option	Description																																				
enable	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.											
add-route	Enable/disable automatic route addition.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Add route according to phase1 add-route setting.</td></tr><tr><td><i>enable</i></td><td>Add route for remote proxy ID.</td></tr><tr><td><i>disable</i></td><td>Do not add route for remote proxy ID.</td></tr></table>	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.			
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.											
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.											
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Send short-cut messages according to the phase1 auto-discovery-sender setting.</td></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>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.											
<i>enable</i>	Enable sending auto-discovery short-cut messages.											
<i>disable</i>	Disable sending auto-discovery short-cut messages.											
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.</td></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>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.											
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.											
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.											

Parameter	Description	Type	Size	Default								
keylifeseconds	Phase2 key life in time in seconds (120 - 172800).	integer	Minimum value: 120 Maximum value: 172800	43200								
keylifekbs	Phase2 key life in number of kilobytes of traffic (5120 - 4294967295).	integer	Minimum value: 5120 Maximum value: 4294967295	5120								
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.											
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.											
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.											
comments	Comment.	var-string	Maximum length: 255									
protocol	Quick mode protocol selector (1 - 255 or 0 for all).	integer	Minimum value: 0 Maximum value: 255	0								
src-name	Local proxy ID name.	string	Maximum length: 79									
src-name6	Local proxy ID name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default																		
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-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-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-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																		
src-port	Quick mode source port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535	0																		
dst-name	Remote proxy ID name.	string	Maximum length: 79																			
dst-name6	Remote proxy ID name.	string	Maximum length: 79																			
dst-addr-type	Remote proxy ID type.	option	-	subnet																		

Parameter	Description	Type	Size	Default																		
	<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.																					
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-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-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																		
dst-port	Quick mode destination port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535	0																		

config vpn qkd

Configure Quantum Key Distribution servers

```

config vpn qkd
  Description: Configure Quantum Key Distribution servers
  edit <name>
    set server {string}
    set port {integer}

```

```

    set id {string}
    set peer {string}
    set certificate <name1>, <name2>, ...
    set comment {var-string}
  next
end

```

config vpn qkd

Parameter	Description	Type	Size	Default
name	Quantum Key Distribution configuration name.	string	Maximum length: 35	
server	IPv4, IPv6 or DNS address of the KME.	string	Maximum length: 63	
port	Port to connect to on the KME.	integer	Minimum value: 1 Maximum value: 65535	0
id	Quantum Key Distribution ID assigned by the KME.	string	Maximum length: 291	
peer	Authenticate Quantum Key Device's certificate with the peer/peergrp.	string	Maximum length: 35	
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	

waf

This section includes syntax for the following commands:

- [config waf main-class on page 1314](#)
- [config waf profile on page 1314](#)
- [config waf signature on page 1339](#)
- [config waf sub-class on page 1340](#)

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
name	Main signature class name.	string	Maximum length: 127	
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config waf profile

Configure Web application firewall configuration.

```
config waf profile
  Description: Configure Web application firewall configuration.
  edit <name>
    set external [disable|enable]
```

```

set extended-log [enable|disable]
config signature
    Description: WAF signatures.
    config main-class
        Description: Main signature class.
        edit <id>
            set status [enable|disable]
            set action [allow|block|...]
            set log [enable|disable]
            set severity [high|medium|...]
        next
    end
    set disabled-sub-class <id1>, <id2>, ...
    set disabled-signature <id1>, <id2>, ...
    set credit-card-detection-threshold {integer}
    config custom-signature
        Description: Custom signature.
        edit <name>
            set status [enable|disable]
            set action [allow|block|...]
            set log [enable|disable]
            set severity [high|medium|...]
            set direction [request|response]
            set case-sensitivity [disable|enable]
            set pattern {string}
            set target {option1}, {option2}, ...
        next
    end
end
config constraint
    Description: WAF HTTP protocol restrictions.
    config header-length
        Description: HTTP header length in request.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config content-length
        Description: HTTP content length in request.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config param-length
        Description: Maximum length of parameter in URL, HTTP POST request or HTTP body.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]

```

```

        set log [enable|disable]
        set severity [high|medium|...]
    end
    config line-length
        Description: HTTP line length in request.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config url-param-length
        Description: Maximum length of parameter in URL.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config version
        Description: Enable/disable HTTP version check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config method
        Description: Enable/disable HTTP method check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config hostname
        Description: Enable/disable hostname check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config malformed
        Description: Enable/disable malformed HTTP request check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-cookie
        Description: Maximum number of cookies in HTTP request.
        set status [enable|disable]
        set max-cookie {integer}
        set action [allow|block]

```



```

        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-header-line
        Description: Maximum number of HTTP header line.
        set status [enable|disable]
        set max-header-line {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-url-param
        Description: Maximum number of parameters in URL.
        set status [enable|disable]
        set max-url-param {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-range-segment
        Description: Maximum number of range segments in HTTP range line.
        set status [enable|disable]
        set max-range-segment {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config exception
        Description: HTTP constraint exception.
        edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}
            set header-length [enable|disable]
            set content-length [enable|disable]
            set param-length [enable|disable]
            set line-length [enable|disable]
            set url-param-length [enable|disable]
            set version [enable|disable]
            set method [enable|disable]
            set hostname [enable|disable]
            set malformed [enable|disable]
            set max-cookie [enable|disable]
            set max-header-line [enable|disable]
            set max-url-param [enable|disable]
            set max-range-segment [enable|disable]
        next
    end
end
config method
    Description: Method restriction.
    set status [enable|disable]

```

```

set log [enable|disable]
set severity [high|medium|...]
set default-allowed-methods {option1}, {option2}, ...
config method-policy
    Description: HTTP method policy.
    edit <id>
        set pattern {string}
        set regex [enable|disable]
        set address {string}
        set allowed-methods {option1}, {option2}, ...
    next
end
end
config address-list
    Description: Address block and allow lists.
    set status [enable|disable]
    set blocked-log [enable|disable]
    set severity [high|medium|...]
    set trusted-address <name1>, <name2>, ...
    set blocked-address <name1>, <name2>, ...
end
config url-access
    Description: URL access list.
    edit <id>
        set address {string}
        set action [bypass|permit|...]
        set log [enable|disable]
        set severity [high|medium|...]
        config access-pattern
            Description: URL access pattern.
            edit <id>
                set srcaddr {string}
                set pattern {string}
                set regex [enable|disable]
                set negate [enable|disable]
            next
        next
    end
next
end
set comment {var-string}
next
end

```

config waf profile

Parameter	Description	Type	Size	Default
name	WAF Profile name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
external	Disable/Enable external HTTP Inspection.	option	-	disable
	Option Description			
	<i>disable</i>	Disable external inspection.		
	<i>enable</i>	Enable external inspection.		
extended-log	Enable/disable extended logging.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
comment	Comment.	var-string	Maximum length: 1023	

config signature

Parameter	Description	Type	Size	Default
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	
disabled-signature <id>	Disabled signatures. Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	
credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 Maximum value: 128	3

config main-class

Parameter	Description	Type	Size	Default
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Status.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	allow	Allow.		
	block	Block.		
	erase	Erase credit card numbers.		
log	Enable/disable logging.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	high	High severity.		
	medium	Medium severity.		
	low	Low severity.		

config custom-signature

Parameter	Description	Type	Size	Default
name	Signature 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.		
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
	<i>erase</i>	Erase credit card numbers.		
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.		
direction	Traffic direction.	option	-	request
	Option	Description		
	<i>request</i>	Match HTTP request.		
	<i>response</i>	Match HTTP response.		
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	<i>disable</i>	Case insensitive in pattern.		
	<i>enable</i>	Case sensitive in pattern.		
pattern	Match pattern.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
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 header-length

Parameter	Description	Type	Size	Default						
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.									
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192						
action	Action.	option	-	allow						

Parameter	Description	Type	Size	Default
	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.		

config content-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	67108864
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	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 param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config line-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024
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.		

config url-param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
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.		

config version

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

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.											
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.											

config method

Parameter	Description	Type	Size	Default						
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.									
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.									
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.									

Parameter	Description	Type	Size	Default
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config hostname

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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.		

config malformed

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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.		

config max-cookie

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	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

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.		

config max-header-line

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	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
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	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 max-url-param

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	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
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config max-range-segment

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	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
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.		

config exception

Parameter	Description	Type	Size	Default						
id	Exception ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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.									
address	Host address.	string	Maximum length: 79							
header-length	HTTP header length in request.	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.									
content-length	HTTP content length in request.	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.									
line-length	HTTP line length in request.	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.		
method	Enable/disable HTTP method check.	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.		
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-header-line	Maximum number of HTTP header line.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-url-param	Maximum number of parameters in URL.	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.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity		
	<i>medium</i>	medium severity		
	<i>low</i>	low severity		
default-allowed-methods	Methods.	option	-	
	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.		

config method-policy

Parameter	Description	Type	Size	Default
id	HTTP method policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
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.		

Parameter	Description	Type	Size	Default
address	Host address.	string	Maximum length: 79	
allowed-methods	Allowed Methods.	option	-	
	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.		

config address-list

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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.		

Parameter	Description	Type	Size	Default
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79	
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	

config url-access

Parameter	Description	Type	Size	Default
id	URL access ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
address	Host address.	string	Maximum length: 79	
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.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	high	High severity.		
	medium	Medium severity.		
	low	Low severity.		

config access-pattern

Parameter	Description	Type	Size	Default						
id	URL access pattern ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
srcaddr	Source address.	string	Maximum length: 79							
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.									
negate	Enable/disable match negation.	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 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
name	Signature subclass name.	string	Maximum length: 127	
id	Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

wanopt

This section includes syntax for the following commands:

- [config wanopt auth-group on page 1341](#)
- [config wanopt cache-service on page 1342](#)
- [config wanopt content-delivery-network-rule on page 1344](#)
- [config wanopt peer on page 1350](#)
- [config wanopt profile on page 1350](#)
- [config wanopt remote-storage on page 1359](#)
- [config wanopt settings on page 1360](#)

config wanopt auth-group

Configure WAN optimization authentication groups.

```
config wanopt auth-group
  Description: Configure WAN optimization authentication groups.
  edit <name>
    set auth-method [cert|psk]
    set psk {password}
    set cert {string}
    set peer-accept [any|defined|...]
    set peer {string}
  next
end
```

config wanopt auth-group

Parameter	Description	Type	Size	Default
name	Auth-group name.	string	Maximum length: 35	
auth-method	Select certificate or pre-shared key authentication for this authentication group.	option	-	cert
		Option	Description	
		cert	Certificate authentication.	
		psk	Pre-shared secret key authentication.	

Parameter	Description	Type	Size	Default								
psk	Pre-shared key used by the peers in this authentication group.	password	Not Specified									
cert	Name of certificate to identify this peer.	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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer that can authenticate with this auth group.</td></tr><tr><td><i>defined</i></td><td>Accept only the peers added with the wanopt peer command.</td></tr><tr><td><i>one</i></td><td>Accept the peer added to this auth group using the peer option.</td></tr></table>				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.
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.											
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									

config wanopt cache-service

Designate cache-service for wan-optimization and webcache.

```

config wanopt cache-service
  Description: Designate cache-service for wan-optimization and webcache.
  set prefer-scenario [balance|prefer-speed|...]
  set collaboration [enable|disable]
  set device-id {string}
  set acceptable-connections [any|peers]
  config dst-peer
    Description: Modify cache-service destination peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set priority {integer}
      set ip {ipv4-address-any}
    next
  end
  config src-peer
    Description: Modify cache-service source peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set priority {integer}
      set ip {ipv4-address-any}
    next

```

```
end
end
```

config wanopt cache-service

Parameter	Description	Type	Size	Default
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.		
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
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.		

config dst-peer

Parameter	Description	Type	Size	Default
device-id	Device ID of this peer.	string	Maximum length: 35	
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

config src-peer

Parameter	Description	Type	Size	Default
device-id	Device ID of this peer.	string	Maximum length: 35	
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt content-delivery-network-rule

Configure WAN optimization content delivery network rules.

```
config wanopt content-delivery-network-rule
    Description: Configure WAN optimization content delivery network rules.
    edit <name>
        set comment {var-string}
```

```

set status [enable|disable]
set host-domain-name-suffix <name1>, <name2>, ...
set category [vcache|youtube]
set request-cache-control [enable|disable]
set response-cache-control [enable|disable]
set response-expires [enable|disable]
set updateserver [enable|disable]
config rules
  Description: WAN optimization content delivery network rule entries.
  edit <name>
    set match-mode [all|any]
    set skip-rule-mode [all|any]
    config match-entries
      Description: List of entries to match.
      edit <id>
        set target [path|parameter|...]
        set pattern <string1>, <string2>, ...
      next
    end
    config skip-entries
      Description: List of entries to skip.
      edit <id>
        set target [path|parameter|...]
        set pattern <string1>, <string2>, ...
      next
    end
    config content-id
      Description: Content ID settings.
      set target [path|parameter|...]
      set start-str {string}
      set start-skip {integer}
      set start-direction [forward|backward]
      set end-str {string}
      set end-skip {integer}
      set end-direction [forward|backward]
      set range-str {string}
    end
  next
end
next
end
end

```

config wanopt content-delivery-network-rule

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
comment	Comment about this CDN-rule.	var-string	Maximum length: 255							
status	Enable/disable WAN optimization content delivery network rules.	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.									
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							
category	Content delivery network rule category.	option	-	vcache						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vcache</i></td><td>Vcache content delivery network.</td></tr><tr><td><i>youtube</i></td><td>Youtube content delivery network.</td></tr></table>	Option	Description	<i>vcache</i>	Vcache content delivery network.	<i>youtube</i>	Youtube content delivery network.			
Option	Description									
<i>vcache</i>	Vcache content delivery network.									
<i>youtube</i>	Youtube content delivery network.									
request-cache-control	Enable/disable HTTP request cache control.	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.									
response-cache-control	Enable/disable HTTP response cache control.	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.									
response-expires	Enable/disable HTTP response cache expires.	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
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
name	WAN optimization content delivery network rule name.	string	Maximum length: 35	
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.		
skip-rule-mode	Skip mode when evaluating skip-rules.	option	-	all
	Option	Description		
	<i>all</i>	Must match all skip entries.		
	<i>any</i>	Must match any skip entries.		

config match-entries

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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	

config skip-entries

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

config content-id

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.		
	start-str	String from which to start search.	string	Maximum length: 35
start-skip	Number of characters in URL to skip after start-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-direction	Search direction from start-str match.	option	-	forward
	Option	Description		
	<i>forward</i>	Forward direction.		
	<i>backward</i>	Backward direction.		
end-str	String from which to end search.	string	Maximum length: 35	
end-skip	Number of characters in URL to skip after end-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0

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.									
range-str	Name of content ID within the start string and end string.	string	Maximum length: 35							

config wanopt peer

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
peer-host-id	Peer host ID.	string	Maximum length: 35	
ip	Peer IP address.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt profile

Configure WAN optimization profiles.

```
config wanopt profile
    Description: Configure WAN optimization profiles.
    edit <name>
        set transparent [enable|disable]
        set comments {var-string}
        set auth-group {string}
    config http
```

```

        Description: Enable/disable HTTP WAN Optimization and configure HTTP WAN Optimization
features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set ssl [enable|disable]
        set prefer-chunking [dynamic|fix]
        set protocol-opt [protocol|tcp]
        set tunnel-sharing [shared|express-shared|...]
    end
    config cifs
        Description: Enable/disable CIFS (Windows sharing) WAN Optimization and configure CIFS
WAN Optimization features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set prefer-chunking [dynamic|fix]
        set protocol-opt [protocol|tcp]
        set tunnel-sharing [shared|express-shared|...]
    end
    config mapi
        Description: Enable/disable MAPI email WAN Optimization and configure MAPI WAN
Optimization features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set tunnel-sharing [shared|express-shared|...]
    end
    config ftp
        Description: Enable/disable FTP WAN Optimization and configure FTP WAN Optimization
features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set prefer-chunking [dynamic|fix]
        set protocol-opt [protocol|tcp]
        set tunnel-sharing [shared|express-shared|...]
    end
    config tcp
        Description: Enable/disable TCP WAN Optimization and configure TCP WAN Optimization
features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set byte-caching-opt [mem-only|mem-disk]
        set tunnel-sharing [shared|express-shared|...]
        set port {user}
        set ssl [enable|disable]
        set ssl-port {user}
    end
next
end

```

config wanopt profile

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 FortiProxy internal interface. Similar to source NAT.		
comments	Comment.	var-string	Maximum length: 255	
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	

config http

Parameter	Description	Type	Size	Default						
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.									
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.									
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.		
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.		
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.		
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 cifs

Parameter	Description	Type	Size	Default						
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.									
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.									
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.									
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 mapi

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN 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.		
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.		
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 ftp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN 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.		
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

Parameter	Description	Type	Size	Default
	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.		
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 tcp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	enable	Enable WAN Optimization.		
	disable	Disable WAN 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								
	<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.											
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	-	disable								
	<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.											
byte-caching-opt	Select whether TCP byte-caching uses system memory only or both memory and disk space.	option	-	mem-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mem-only</i></td><td>Byte caching with memory only.</td></tr><tr><td><i>mem-disk</i></td><td>Byte caching with memory and disk.</td></tr></table>	Option	Description	<i>mem-only</i>	Byte caching with memory only.	<i>mem-disk</i>	Byte caching with memory and disk.					
	Option	Description										
	<i>mem-only</i>	Byte caching with memory only.										
<i>mem-disk</i>	Byte caching with memory and disk.											
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.											
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									
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	

config wanopt remote-storage

Configure a remote cache device as Web cache storage.

```
config wanopt remote-storage
  Description: Configure a remote cache device as Web cache storage.
  set status [disable|enable]
  set local-cache-id {string}
  set remote-cache-id {string}
  set remote-cache-ip {ipv4-address-any}
end
```

config wanopt remote-storage

Parameter	Description	Type	Size	Default
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.		
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	
remote-cache-ip	IP address of the remote device to which the device connects.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt settings

Configure WAN optimization settings.

```
config wanopt settings
  Description: Configure WAN optimization settings.
  set host-id {string}
  set tunnel-ssl-algorithm [high|medium|...]
  set auto-detect-algorithm [simple|diff-req-resp]
  set tunnel-optimization [memory-usage|balanced|...]
end
```

config wanopt settings

Parameter	Description	Type	Size	Default								
host-id	Local host ID (must also be entered in the remote FortiProxy's peer list).	string	Maximum length: 35	default-id								
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>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.											
auto-detect-algorithm	Auto detection algorithms used in tunnel negotiations.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>simple</td><td>Use the same TCP option value in SYN/SYNACK packets. Backward compatible.</td></tr><tr><td>diff-req-resp</td><td>Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.</td></tr></table>	Option	Description	simple	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.	diff-req-resp	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.					
Option	Description											
simple	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.											
diff-req-resp	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.											
tunnel-optimization	WANOpt tunnel optimization option.	option	-	balanced								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>memory-usage</td><td>Optimize tunnel for low system memory usage.</td></tr><tr><td>balanced</td><td>Optimize tunnel to balance between system memory usage and throughput.</td></tr><tr><td>throughput</td><td>Optimize tunnel for throughput.</td></tr></table>	Option	Description	memory-usage	Optimize tunnel for low system memory usage.	balanced	Optimize tunnel to balance between system memory usage and throughput.	throughput	Optimize tunnel for throughput.			
Option	Description											
memory-usage	Optimize tunnel for low system memory usage.											
balanced	Optimize tunnel to balance between system memory usage and throughput.											
throughput	Optimize tunnel for throughput.											

web-proxy

This section includes syntax for the following commands:

- [config web-proxy debug-url on page 1361](#)
- [config web-proxy dynamic-bypass on page 1362](#)
- [config web-proxy explicit-proxy on page 1363](#)
- [config web-proxy fast-fallback on page 1370](#)
- [config web-proxy forward-server-group on page 1373](#)
- [config web-proxy forward-server on page 1371](#)
- [config web-proxy global on page 1375](#)
- [config web-proxy implicit-proxy-rule on page 1381](#)
- [config web-proxy implicit-proxy-setting on page 1382](#)
- [config web-proxy isolator-server on page 1383](#)
- [config web-proxy pac-policy on page 1384](#)
- [config web-proxy profile on page 1385](#)
- [config web-proxy redirect-profile on page 1390](#)
- [config web-proxy url-list on page 1392](#)
- [config web-proxy url-match on page 1393](#)
- [config web-proxy wisp on page 1394](#)

config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
  Description: Configure debug URL addresses.
  edit <name>
    set url-pattern {string}
    set status [enable|disable]
    set exact [enable|disable]
  next
end
```

config web-proxy debug-url

Parameter	Description	Type	Size	Default
name	Debug URL name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
url-pattern	URL exemption pattern.	string	Maximum length: 511							
status	Enable/disable this URL exemption.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this URL exemption.</td></tr><tr><td><i>disable</i></td><td>Disable this URL exemption.</td></tr></table>	Option	Description	<i>enable</i>	Enable this URL exemption.	<i>disable</i>	Disable this URL exemption.			
Option	Description									
<i>enable</i>	Enable this URL exemption.									
<i>disable</i>	Disable this URL exemption.									
exact	Enable/disable matching the exact path.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable matching the exact path.</td></tr><tr><td><i>disable</i></td><td>Disable matching the exact path.</td></tr></table>	Option	Description	<i>enable</i>	Enable matching the exact path.	<i>disable</i>	Disable matching the exact path.			
Option	Description									
<i>enable</i>	Enable matching the exact path.									
<i>disable</i>	Disable matching the exact path.									

config web-proxy dynamic-bypass

Configure dynamic bypass settings.

```

config web-proxy dynamic-bypass
    Description: Configure dynamic bypass settings.
    set status [enable|disable]
    set errors {option1}, {option2}, ...
    set total-max {integer}
    set server-max {integer}
    set timeout {integer}
end

```

config web-proxy dynamic-bypass

Parameter	Description	Type	Size	Default
status	Enable/disable dynamic bypass.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dynamic bypass.		
	<i>disable</i>	Disable dynamic bypass.		
errors	Configure bypass errors.	option	-	

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>connect-error</i></td><td>Connect error.</td></tr><tr><td><i>receive-error</i></td><td>HTTP response is not received.</td></tr><tr><td><i>non-http</i></td><td>HTTP protocol is not detected.</td></tr><tr><td><i>400</i></td><td>HTTP response code is 400.</td></tr><tr><td><i>401</i></td><td>HTTP response code is 401.</td></tr><tr><td><i>403</i></td><td>HTTP response code is 403.</td></tr><tr><td><i>405</i></td><td>HTTP response code is 405.</td></tr><tr><td><i>406</i></td><td>HTTP response code is 406.</td></tr><tr><td><i>500</i></td><td>HTTP response code is 500.</td></tr><tr><td><i>502</i></td><td>HTTP response code is 502.</td></tr><tr><td><i>503</i></td><td>HTTP response code is 503.</td></tr><tr><td><i>504</i></td><td>HTTP response code is 504.</td></tr></table>	Option	Description	<i>connect-error</i>	Connect error.	<i>receive-error</i>	HTTP response is not received.	<i>non-http</i>	HTTP protocol is not detected.	<i>400</i>	HTTP response code is 400.	<i>401</i>	HTTP response code is 401.	<i>403</i>	HTTP response code is 403.	<i>405</i>	HTTP response code is 405.	<i>406</i>	HTTP response code is 406.	<i>500</i>	HTTP response code is 500.	<i>502</i>	HTTP response code is 502.	<i>503</i>	HTTP response code is 503.	<i>504</i>	HTTP response code is 504.			
	Option	Description																												
	<i>connect-error</i>	Connect error.																												
	<i>receive-error</i>	HTTP response is not received.																												
	<i>non-http</i>	HTTP protocol is not detected.																												
	<i>400</i>	HTTP response code is 400.																												
	<i>401</i>	HTTP response code is 401.																												
	<i>403</i>	HTTP response code is 403.																												
	<i>405</i>	HTTP response code is 405.																												
	<i>406</i>	HTTP response code is 406.																												
	<i>500</i>	HTTP response code is 500.																												
	<i>502</i>	HTTP response code is 502.																												
	<i>503</i>	HTTP response code is 503.																												
<i>504</i>	HTTP response code is 504.																													
total-max	Maximum numbers of entries in dynamic bypass list (10 - 50000, default = 5000).	integer	Minimum value: 10 Maximum value: 50000	5000																										
server-max	Maximum numbers of entries in dynamic bypass list belongs to one server, all requests to this server will be bypassed once server-max is reached (1 - 255, default = 16).	integer	Minimum value: 1 Maximum value: 255	16																										
timeout	Maximum time (in minutes) that an entry is kept in dynamic bypass list from its last hit (1 - 21600, default = 60).	integer	Minimum value: 1 Maximum value: 21600	60																										

config web-proxy explicit-proxy

Configure explicit Web proxy settings.

```
config web-proxy explicit-proxy
  Description: Configure explicit Web proxy settings.
  edit <name>
    set status [enable|disable]
    set interface {string}
```

```

set secure-web-proxy [disable|enable|...]
set http [enable|disable]
set ftp-over-http [enable|disable]
set socks [enable|disable]
set http-incoming-port {user}
set http-connection-mode [static|multiplex|...]
set https-incoming-port {user}
set ftp-incoming-port {user}
set socks-incoming-port {user}
set secure-web-proxy-cert <name1>, <name2>, ...
set client-cert [disable|enable]
set user-agent-detect [disable|enable]
set empty-cert-action [accept|block|...]
set ssl-dh-bits [768|1024|...]
set incoming-ip {ipv4-address-any}
set ipv6-status [enable|disable]
set incoming-ip6 {ipv6-address}
set pref-dns-result [ipv4|ipv6|...]
set unknown-http-version [reject|best-effort]
set realm {string}
set sec-default-action [accept|deny]
set pac-file-server-status [enable|disable]
set pac-file-url {user}
set pac-file-server-port {user}
set pac-file-through-https [enable|disable]
set pac-file-name {string}
set pac-file-data {user}
set ssl-algorithm [high|medium|...]
set return-to-sender [enable|disable]
set learn-dst-from-sni [enable|disable]
set dstport-from-incoming [enable|disable]
set header-proxy-agent [enable|disable]
set dns-mode [recursive|non-recursive|...]
next
end

```

config web-proxy explicit-proxy

Parameter	Description	Type	Size	Default
name	object name	string	Maximum length: 35	
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								
interface	interface name	string	Maximum length: 15									
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><i>disable</i></td><td>Disable secure webproxy.</td></tr><tr><td><i>enable</i></td><td>Enable secure webproxy access.</td></tr><tr><td><i>secure</i></td><td>Require secure webproxy access.</td></tr></table>	Option	Description	<i>disable</i>	Disable secure webproxy.	<i>enable</i>	Enable secure webproxy access.	<i>secure</i>	Require secure webproxy access.			
Option	Description											
<i>disable</i>	Disable secure webproxy.											
<i>enable</i>	Enable secure webproxy access.											
<i>secure</i>	Require secure webproxy access.											
http	Enable/disable the HTTP & HTTPS proxy.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the HTTP & HTTPS proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the HTTP & HTTPS proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the HTTP & HTTPS proxy.	<i>disable</i>	Disable the HTTP & HTTPS proxy.					
Option	Description											
<i>enable</i>	Enable the HTTP & HTTPS proxy.											
<i>disable</i>	Disable the HTTP & HTTPS proxy.											
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable								
	<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.											
socks	Enable/disable the SOCKS proxy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the SOCKS proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the SOCKS proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the SOCKS proxy.	<i>disable</i>	Disable the SOCKS proxy.					
Option	Description											
<i>enable</i>	Enable the SOCKS proxy.											
<i>disable</i>	Disable the SOCKS proxy.											
http-incoming-port	Accept incoming HTTP requests on one or more ports (0 - 65535, default = 8080).	user	Not Specified									
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.											

Parameter	Description	Type	Size	Default								
https-incoming-port	Accept incoming HTTPS requests on one or more ports (0 - 65535, default = 0, use the same as HTTP).	user	Not Specified									
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									
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									
secure-web-proxy-cert <name>	Name of certificates for secure web proxy. Certificate list.	string	Maximum length: 79									
client-cert	Enable/disable to request client certificate.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable client certificate request.</td></tr><tr><td><i>enable</i></td><td>Enable client certificate request.</td></tr></table>	Option	Description	<i>disable</i>	Disable client certificate request.	<i>enable</i>	Enable client certificate request.					
Option	Description											
<i>disable</i>	Disable client certificate request.											
<i>enable</i>	Enable client certificate request.											
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.											
empty-cert-action	Action of an empty client certificate.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>block</i></td><td>Block the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>accept-unmanageable</i></td><td>Accept the SSL handshake only if the end-point is unmanageable.</td></tr></table>	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.			
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.											
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-	2048								

Parameter	Description	Type	Size	Default										
	<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></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.			
	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.													
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										
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>enable</td><td>Enable allowing an IPv6 web proxy destination.</td></tr><tr><td>disable</td><td>Disable allowing an IPv6 web proxy destination.</td></tr></table>	Option	Description	enable	Enable allowing an IPv6 web proxy destination.	disable	Disable allowing an IPv6 web proxy destination.							
	Option	Description												
	enable	Enable allowing an IPv6 web proxy destination.												
disable	Disable allowing an IPv6 web proxy destination.													
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	::										
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.													
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject										

Parameter	Description	Type	Size	Default
	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.		
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
	Option	Description		
	<i>accept</i>	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.		
	<i>deny</i>	Deny requests unless there is a matching explicit web proxy policy.		
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Proxy Auto-Configuration (PAC).		
	<i>disable</i>	Disable Proxy Auto-Configuration (PAC).		
pac-file-url	PAC file access URL.	user	Not Specified	
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-through-https	Enable/disable to get Proxy Auto-Configuration (PAC) through HTTPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable to get Proxy Auto-Configuration (PAC) through HTTPS.		
	<i>disable</i>	Disable to get Proxy Auto-Configuration (PAC) through HTTPS.		

Parameter	Description	Type	Size	Default								
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac								
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified									
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-	low								
	<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.											
return-to-sender	Enable/disable return-to-sender.	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-dst-from-sni	Enable/disable learning destination from SNI in client hello.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable learning destination from SNI in client hello.</td></tr><tr><td><i>disable</i></td><td>Disable learning destination from SNI in client hello.</td></tr></table>	Option	Description	<i>enable</i>	Enable learning destination from SNI in client hello.	<i>disable</i>	Disable learning destination from SNI in client hello.					
Option	Description											
<i>enable</i>	Enable learning destination from SNI in client hello.											
<i>disable</i>	Disable learning destination from SNI in client hello.											
dstport-from-incoming	Enable/disable reusing incoming port to connect to server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reusing incoming port to connect to server.</td></tr><tr><td><i>disable</i></td><td>Disable reusing incoming port to connect to server.</td></tr></table>	Option	Description	<i>enable</i>	Enable reusing incoming port to connect to server.	<i>disable</i>	Disable reusing incoming port to connect to server.					
Option	Description											
<i>enable</i>	Enable reusing incoming port to connect to server.											
<i>disable</i>	Disable reusing incoming port to connect to server.											
header-proxy-agent	Enable/disable HTTP CONNECT response header Proxy-Agent.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP CONNECT response header Proxy-Agent.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP CONNECT response header Proxy-Agent.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP CONNECT response header Proxy-Agent.	<i>disable</i>	Disable HTTP CONNECT response header Proxy-Agent.					
Option	Description											
<i>enable</i>	Enable HTTP CONNECT response header Proxy-Agent.											
<i>disable</i>	Disable HTTP CONNECT response header Proxy-Agent.											

Parameter	Description	Type	Size	Default
dns-mode	DNS lookup mode (default=recursive).	option	-	recursive
	Option	Description		
	<i>recursive</i>	Shadow DNS database and forward.		
	<i>non-recursive</i>	Public DNS database only.		
	<i>forward-only</i>	Forward only.		

config web-proxy fast-fallback

Proxy destination connection fast-fallback.

```

config web-proxy fast-fallback
  Description: Proxy destination connection fast-fallback.
  edit <name>
    set status [enable|disable]
    set connection-mode [sequentially|simultaneously]
    set protocol [IPv4-first|IPv6-first|...]
    set connection-timeout {integer}
  next
end

```

config web-proxy fast-fallback

Parameter	Description	Type	Size	Default
name	Configure a name for the fast-fallback entry.	string	Maximum length: 63	
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.		
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.		

Parameter	Description	Type	Size	Default
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.		
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

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 ip {ipv4-address-any}
    set ipv6 {ipv6-address}
    set fqdn {string}
    set port {integer}
    set comment {string}
    set masquerade [enable|disable]
    set protocol {option1}, {option2}, ...
    set ippool <name1>, <name2>, ...
    set healthcheck [disable|enable]
    set monitor {string}
    set server-down-option [block|pass]
    set username {string}
    set password {password}
  next
end

```

config web-proxy forward-server

Parameter	Description	Type	Size	Default								
name	Server name.	string	Maximum length: 63									
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ip</td><td>Use an IPv4 address for the forwarding proxy server.</td></tr><tr><td>ipv6</td><td>Use an IPv6 address for the forwarding proxy server.</td></tr><tr><td>fqdn</td><td>Use the FQDN for the forwarding proxy server.</td></tr></table>				Option	Description	ip	Use an IPv4 address for the forwarding proxy server.	ipv6	Use an IPv6 address for the forwarding proxy server.	fqdn	Use the FQDN for the forwarding proxy server.
	Option	Description										
	ip	Use an IPv4 address for the forwarding proxy server.										
	ipv6	Use an IPv6 address for the forwarding proxy server.										
fqdn	Use the FQDN for the forwarding proxy server.											
ip	Forward proxy server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0								
ipv6	Forward proxy server IPv6 address.	ipv6-address	Not Specified	::								
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255									
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								
comment	Comment.	string	Maximum length: 63									
masquerade	set webproxy to use device address to connect proxy server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable using device address to connect proxy server.</td></tr><tr><td>disable</td><td>Disable using device address to connect proxy server.</td></tr></table>				Option	Description	enable	Enable using device address to connect proxy server.	disable	Disable using device address to connect proxy server.		
	Option	Description										
	enable	Enable using device address to connect proxy server.										
disable	Disable using device address to connect proxy server.											
protocol	Supported proxy protocols.	option	-	http socks								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>Support forwarding through HTTP proxy.</td></tr><tr><td>socks</td><td>Support forwarding through SOCKS.</td></tr><tr><td>ftp</td><td>Support forwarding through FTP proxy.</td></tr></table>				Option	Description	http	Support forwarding through HTTP proxy.	socks	Support forwarding through SOCKS.	ftp	Support forwarding through FTP proxy.
	Option	Description										
	http	Support forwarding through HTTP proxy.										
	socks	Support forwarding through SOCKS.										
ftp	Support forwarding through FTP proxy.											

Parameter	Description	Type	Size	Default						
ippool <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79							
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						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable health checking.</td></tr><tr><td><i>enable</i></td><td>Enable health checking.</td></tr></table>				Option	Description	<i>disable</i>	Disable health checking.	<i>enable</i>	Enable health checking.
Option	Description									
<i>disable</i>	Disable health checking.									
<i>enable</i>	Enable health checking.									
monitor	URL for forward server health check monitoring (default = www.google.com).	string	Maximum length: 255	www.google.com						
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><i>block</i></td><td>Block sessions until the server is back up.</td></tr><tr><td><i>pass</i></td><td>Pass sessions to their destination bypassing the forward server.</td></tr></table>				Option	Description	<i>block</i>	Block sessions until the server is back up.	<i>pass</i>	Pass sessions to their destination bypassing the forward server.
Option	Description									
<i>block</i>	Block sessions until the server is back up.									
<i>pass</i>	Pass sessions to their destination bypassing the forward server.									
username	HTTP authentication user name.	string	Maximum length: 64							
password	HTTP authentication password.	password	Not Specified							

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 ldb-method [weighted|least-session|...]
```

```

    set group-down-option [block|pass]
    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								
name	Configure a forward server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63									
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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable affinity.</td></tr><tr><td><i>disable</i></td><td>Disable affinity.</td></tr></table>	Option	Description	<i>enable</i>	Enable affinity.	<i>disable</i>	Disable affinity.					
Option	Description											
<i>enable</i>	Enable affinity.											
<i>disable</i>	Disable affinity.											
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.											
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								

Parameter	Description	Type	Size	Default
	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.		

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 ssl-cert {string}
  set ssl-ca-cert {string}
  set fast-policy-match [enable|disable]
  set ldap-user-cache [enable|disable]
  set proxy-fqdn {string}
  set max-request-length {integer}
  set max-message-length {integer}
  set strict-web-check [enable|disable]
  set forward-proxy-auth [enable|disable]
  set forward-server-affinity-timeout {integer}
  set webproxy-profile {string}
  set learn-client-ip [disable|traffic-process|...]
  set always-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 src-affinity-exempt-addr {ipv4-address-any}
  set src-affinity-exempt-addr6 {ipv6-address}
  set strict-guest [enable|disable]
  set https-replacement-message [enable|disable]
  set message-upon-server-error [enable|disable]
  set trace-auth-no-rsp [enable|disable]
```

```

set log-policy-pending [enable|disable]
set log-forward-server [enable|disable]
set extended-log [enable|disable]
set log-http-transaction [disable|enable]
set log-app-id [enable|disable]
set proxy-transparent-cert-inspection [enable|disable]
set request-obs-fold [replace-with-sp|block|...]
set explicit-outgoing-ip {ipv4-address-any}
set explicit-outgoing-ip6 {ipv6-address}
set realm {string}
end

```

config web-proxy global

Parameter	Description	Type	Size	Default
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	default-server-cert
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	default-ca
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ldap-user-cache	Enable/disable ldap user cache for explicit and transparent proxy user.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
proxy-fqdn	Fully Qualified Domain Name (FQDN) that clients connect to (default = default.fqdn) to connect to the explicit web proxy.	string	Maximum length: 255	default.fqdn
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-message-length	Maximum length of HTTP message, not including body (16 - 256 Kbytes, default = 32).	integer	Minimum value: 16 Maximum value: 256	32								
strict-web-check	Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP 1.1.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict web checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict web checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict web checking.	<i>disable</i>	Disable strict web checking.					
Option	Description											
<i>enable</i>	Enable strict web checking.											
<i>disable</i>	Disable strict web checking.											
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-	disable								
	<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								
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									
learn-client-ip	Learn the client's IP address from headers.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not learn the client's IP address from headers.</td></tr><tr><td><i>traffic-process</i></td><td>Learn the client's IP address from headers and use it for both policy-matching and logging.</td></tr><tr><td><i>log-only</i></td><td>Learn the client's IP address from headers and use it only for logging.</td></tr></table>	Option	Description	<i>disable</i>	Do not learn the client's IP address from headers.	<i>traffic-process</i>	Learn the client's IP address from headers and use it for both policy-matching and logging.	<i>log-only</i>	Learn the client's IP address from headers and use it only for logging.			
Option	Description											
<i>disable</i>	Do not learn the client's IP address from headers.											
<i>traffic-process</i>	Learn the client's IP address from headers and use it for both policy-matching and logging.											
<i>log-only</i>	Learn the client's IP address from headers and use it only for logging.											
always-learn-client-ip	Enable/disable learning the client's IP address from headers for every request.	option	-	disable								

Parameter	Description	Type	Size	Default								
	<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.											
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><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>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.	<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For 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.										
<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									
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									
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.											
https-replacement-message	Default action to enable or disable return 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.											

Parameter	Description	Type	Size	Default						
message-upon-server-error	Enable/disable return of replacement message upon server error detection.	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.									
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.									
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.									
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.									
extended-log	Enable/disable extended log of http transaction for implicit policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging extended http information for implicit policy.</td></tr><tr><td><i>disable</i></td><td>Disable logging extended http information for implicit policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging extended http information for implicit policy.	<i>disable</i>	Disable logging extended http information for implicit policy.			
Option	Description									
<i>enable</i>	Enable logging extended http information for implicit policy.									
<i>disable</i>	Disable logging extended http information for implicit policy.									
log-http-transaction	Enable/disable http transaction log for implicit policy.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable HTTP transaction log.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP transaction log</td></tr></table>	Option	Description	<i>disable</i>	Disable HTTP transaction log.	<i>enable</i>	Enable HTTP transaction log					
	Option	Description										
	<i>disable</i>	Disable HTTP transaction log.										
<i>enable</i>	Enable HTTP transaction log											
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.											
proxy-transparent-cert-inspection	Enable/disable transparent proxy certificate inspection.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable proxying certificate inspection in transparent mode.</td></tr><tr><td><i>disable</i></td><td>Disable proxying certificate inspection in transparent mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable proxying certificate inspection in transparent mode.	<i>disable</i>	Disable proxying certificate inspection in transparent mode.					
	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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>replace-with-sp</i></td><td>Replace CRLF in obs-fold with SP in the request header for HTTP/1.x.</td></tr><tr><td><i>block</i></td><td>Block HTTP/1.x request with obs-fold.</td></tr><tr><td><i>keep</i></td><td>Keep obs-fold in the request header for HTTP/1.x. There are known security risks.</td></tr></table>	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.			
	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.											
explicit-outgoing-ip	Outgoing HTTP requests by explicit webproxy will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified									
explicit-outgoing-ip6	Outgoing HTTP requests by explicit webproxy will leave this IP. An interface must have this IP address.	ipv6-address	Not Specified									
realm	Authentication realm.	string	Maximum length: 63	default								

config web-proxy implicit-proxy-rule

Configure implicit webproxy rule.

```
config web-proxy implicit-proxy-rule
  Description: Configure implicit webproxy rule.
  edit <name>
    set load-balance-method [static|round-robin|...]
    set bypass-list <name1>, <name2>, ...
  config proxy-servers
    Description: Rule proxy server entries.
    edit <id>
      set ip {ipv4-address-any}
      set port {integer}
      set weight {integer}
    next
  end
next
end
```

config web-proxy implicit-proxy-rule

Parameter	Description	Type	Size	Default
name	Rule name.	string	Maximum length: 63	
load-balance-method	Method used to distribute sessions to proxies.	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.	
		<i>first-alive</i>	Distribute to the first server that is alive.	
		<i>weighted</i>	Distribute to server based on weight.	
bypass-list <name>	Addresses for which you do not want to use any proxy Address name.	string	Maximum length: 79	

config proxy-servers

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Proxy IP address.	ipv4-address-any	Not Specified	0.0.0.0
port	Proxy port number (1 - 65535, default = 8080).	integer	Minimum value: 1 Maximum value: 65535	8080
weight	Weight of the proxy 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 web-proxy implicit-proxy-setting

Configure implicit proxy browser extension setting.

```
config web-proxy implicit-proxy-setting
  Description: Configure implicit proxy browser extension setting.
  edit <name>
    set interface {string}
    set implicit-proxy-rule {string}
  next
end
```

config web-proxy implicit-proxy-setting

Parameter	Description	Type	Size	Default
name	object name	string	Maximum length: 35	
interface	interface name	string	Maximum length: 15	
implicit-proxy-rule	Implicit proxy rule name	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 ip {ipv4-address-any}
    set ipv6 {ipv6-address}
    set fqdn {string}
    set port {integer}
    set comment {string}
    set masquerade [enable|disable]
    set protocol {option1}, {option2}, ...
    set ippool <name1>, <name2>, ...
  next
end
```

config web-proxy isolator-server

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 63	
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.		
ip	Forward proxy server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	Forward proxy server IPv6 address.	ipv6-address	Not Specified	::
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
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						
comment	Comment.	string	Maximum length: 63							
masquerade	set webproxy to use device address to connect proxy server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using device address to connect proxy server.</td></tr><tr><td><i>disable</i></td><td>Disable using device address to connect proxy server.</td></tr></table>				Option	Description	<i>enable</i>	Enable using device address to connect proxy server.	<i>disable</i>	Disable using device address to connect proxy server.
Option	Description									
<i>enable</i>	Enable using device address to connect proxy server.									
<i>disable</i>	Disable using device address to connect proxy server.									
protocol	Supported proxy protocols.	option	-	http socks						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Support forwarding through HTTP proxy.</td></tr><tr><td><i>socks</i></td><td>Support forwarding through SOCKS.</td></tr></table>				Option	Description	<i>http</i>	Support forwarding through HTTP proxy.	<i>socks</i>	Support forwarding through SOCKS.
Option	Description									
<i>http</i>	Support forwarding through HTTP proxy.									
<i>socks</i>	Support forwarding through SOCKS.									
ippool <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79							

config web-proxy pac-policy

Configure explicit Web proxy pac policy.

```

config web-proxy pac-policy
  Description: Configure explicit Web proxy pac policy.
  edit <policyid>
    set status [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set pac-file-name {string}
    set pac-file-data {user}
    set comments {var-string}
  next
end

```

config web-proxy pac-policy

Parameter	Description	Type	Size	Default
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 100	0
status	Enable/disable policy.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable policy.	
	<i>disable</i>		Disable policy.	
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
comments	Optional comments.	var-string	Maximum length: 1023	

config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
  Description: Configure web proxy profiles.
  edit <name>
    set max-cache-object-size {integer}
    set header-client-ip [pass|add|...]
    set header-via-request [pass|add|...]
    set header-via-response [pass|add|...]
    set header-x-forwarded-for [pass|add|...]
    set header-x-forwarded-client-cert [pass|add|...]
    set header-front-end-https [pass|add|...]
    set header-x-authenticated-user [pass|add|...]
```

```

set header-x-authenticated-groups [pass|add|...]
set strip-encoding [enable|disable]
set log-header-change [enable|disable]
config headers
    Description: Configure HTTP forwarded requests headers.
    edit <id>
        set name {string}
        set dstaddr <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set action [add-to-request|add-to-response|...]
        set content {string}
        set base64-encoding [disable|enable]
        set add-option [append|new-on-not-found|...]
        set protocol {option1}, {option2}, ...
    next
end
next
end

```

config web-proxy profile

Parameter	Description	Type	Size	Default								
name	Profile name.	string	Maximum length: 63									
max-cache-object-size	Maximum cacheable object size in KB (0-3984384 KB (3.8 GB), default = 0.). When the value is set to 0, the max cache object size will be max-object-size under webcache settings.	integer	Minimum value: 0 Maximum value: 3984384	0								
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-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								

Parameter	Description	Type	Size	Default								
	<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-via-response	Action to take on the HTTP via header in forwarded responses: 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.											
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-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-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.		
	<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.		
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable
	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.		
log-header-change	Enable/disable logging HTTP header changes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Enable/disable logging HTTP header changes.		
	<i>disable</i>	Disable Enable/disable logging HTTP header changes.		

config headers

Parameter	Description	Type	Size	Default														
id	HTTP forwarded header id.	integer	Minimum value: 0 Maximum value: 4294967295	0														
name	HTTP forwarded header name.	string	Maximum length: 79															
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															
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.																	
content	HTTP header content.	string	Maximum length: 3999															
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												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of base64 encoding of HTTP content.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of base64 encoding of HTTP content.											
	Option	Description														
<i>enable</i>	Enable use of base64 encoding of HTTP content.															
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.															
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><i>https</i></td><td>Perform add-option action on HTTPS.</td></tr><tr><td><i>http</i></td><td>Perform add-option action on HTTP.</td></tr></table>	Option	Description	<i>https</i>	Perform add-option action on HTTPS.	<i>http</i>	Perform add-option action on HTTP.									
	Option	Description														
<i>https</i>	Perform add-option action on HTTPS.															
<i>http</i>	Perform add-option action on HTTP.															

config web-proxy redirect-profile

URL redirect profile.

```

config web-proxy redirect-profile
  Description: URL redirect profile.
  edit <name>
    config entries
      Description: URL redirect entries.
      edit <id>
        set type [simple|regex|...]
        set url {var-string}
        set redirect-url {var-string}
        set redirect-code [auto|301|...]
      next
    end
  end

```

```
next
end
```

config web-proxy redirect-profile

Parameter	Description	Type	Size	Default
name	Name of the redirect profile.	string	Maximum length: 35	

config entries

Parameter	Description	Type	Size	Default
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	URL match type (simple, regex or wildcard).	option	-	simple
	Option	Description		
	simple	Simple URL string.		
	regex	Regular expression URL string.		
	wildcard	Wildcard URL string.		
url	URL to be redirected.	var-string	Maximum length: 1023	
redirect-url	Redirect URL for further web proxy processing.	var-string	Maximum length: 1023	
redirect-code	Redirect code.	option	-	auto
	Option	Description		
	auto	Auto select status code.		
	301	Status code 301 Move Permanently.		
	302	Status code 302 Move.		
	303	Status code 303 See Other.		
	307	Status code 307 Temporary Redirect.		
	308	Status code 308 Permanent Redirect.		

config web-proxy url-list

URLs for web proxy.

```
config web-proxy url-list
  Description: URLs for web proxy.
  edit <name>
    set comment {var-string}
    config entries
      Description: URL list entries.
      edit <id>
        set status [enable|disable]
        set url {string}
        set type [simple|wildcard]
      next
    end
  next
end
```

config web-proxy url-list

Parameter	Description	Type	Size	Default
name	Configure a name for the URL list.	string	Maximum length: 63	
comment	Comment.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default						
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable the entry.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable The URL.</td></tr><tr><td><i>disable</i></td><td>Disable The URL.</td></tr></table>				Option	Description	<i>enable</i>	Enable The URL.	<i>disable</i>	Disable The URL.
	Option	Description								
	<i>enable</i>	Enable The URL.								
<i>disable</i>	Disable The URL.									
url	URL.	string	Maximum length: 511							

Parameter	Description	Type	Size	Default						
type	URL type (simple, wildcard).	option	-	simple						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple URL string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard URL string (only '*').</td></tr></table>				Option	Description	<i>simple</i>	Simple URL string.	<i>wildcard</i>	Wildcard URL string (only '*').
Option	Description									
<i>simple</i>	Simple URL string.									
<i>wildcard</i>	Wildcard URL string (only '*').									

config web-proxy url-match

URLs to be exempted from caching and/or to be redirected to forward server.

```

config web-proxy url-match
  Description: URLs to be exempted from caching and/or to be redirected to forward server.
  edit <name>
    set status [enable|disable]
    set explicit-web-proxy <name1>, <name2>, ...
    set type [simple|wildcard|...]
    set url-pattern {string}
    set url-list {string}
    set forward-server {string}
    set ftp-forward-server {string}
    set fast-fallback {string}
    set cache-exemption [enable|disable]
    set comment {var-string}
  next
end

```

config web-proxy url-match

Parameter	Description	Type	Size	Default						
name	Configure a name for the URL to be exempted.	string	Maximum length: 63							
status	Enable/disable URLs to be exempted from caching and/or to be redirected to forward server.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable exempting the matching URLs.</td></tr><tr><td>disable</td><td>Disable exempting the matching URLs.</td></tr></table>				Option	Description	enable	Enable exempting the matching URLs.	disable	Disable exempting the matching URLs.
Option	Description									
enable	Enable exempting the matching URLs.									
disable	Disable exempting the matching URLs.									
explicit-web-proxy <name>	Explicit Web proxy names. Explicit Web proxy name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default
type	URL type (simple, wildcard, list).	option	-	simple
	Option	Description		
	<i>simple</i>	Simple URL string.		
	<i>wildcard</i>	Wildcard URL string (only '*').		
	<i>list</i>	URL list.		
url-pattern	URL pattern to be exempted from caching and/or to be redirected to forward server.	string	Maximum length: 511	
url-list	URL list to be exempted from caching and/or to be redirected to forward server.	string	Maximum length: 63	
forward-server	Forward server name.	string	Maximum length: 63	
ftp-forward-server	ftp forward server name.	string	Maximum length: 63	
fast-fallback	Fast fallback configuration entry name.	string	Maximum length: 63	
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	

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 outgoing-ip {ipv4-address-any}
    set server-ip {ipv4-address-any}
    set server-port {integer}
    set max-connections {integer}
    set timeout {integer}
  next
end

```

config web-proxy wisp

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
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
max-connections	Maximum number of web proxy WISP connections (4 - 4096, default = 64).	integer	Minimum value: 4 Maximum value: 4096	64
timeout	Period of time before WISP requests time out (1 - 15 sec, default = 5).	integer	Minimum value: 1 Maximum value: 15	5

webcache

This section includes syntax for the following commands:

- [config webcache prefetch on page 1396](#)
- [config webcache reverse-cache-server on page 1397](#)
- [config webcache settings on page 1398](#)
- [config webcache user-agent on page 1402](#)

config webcache prefetch

Configure cache prefetch.

```
config webcache prefetch
  Description: Configure cache prefetch.
  edit <name>
    set url {string}
    set crawl-depth {integer}
    set ignore-robots [enable|disable]
    set interval {integer}
    set start-delay {integer}
    set repeat {integer}
    set user {string}
    set password {password}
    set user-agent <name1>, <name2>, ...
  next
end
```

config webcache prefetch

Parameter	Description	Type	Size	Default
name	Name of the prefetch item.	string	Maximum length: 35	
url	URL of the target.	string	Maximum length: 1023	
crawl-depth	Depth(0-16) to crawl the whole url.	integer	Minimum value: 0 Maximum value: 16	0

Parameter	Description	Type	Size	Default
ignore-robots	Ignore robots.txt specification.	option	-	disable
	Option	Description		
	<i>enable</i>	Ignore robots.txt config while crawling the url.		
	<i>disable</i>	Obey robots.txt config while crawling the url.		
interval	Time interval (in seconds) to fetch the url.	integer	Minimum value: 0 Maximum value: 608400	43200
start-delay	Delay period to start the fetching (in secondss).	integer	Minimum value: 0 Maximum value: 2422800	0
repeat	How many times repeat to fetch the url (0 - 4,200,000,000).	integer	Minimum value: 0 Maximum value: 4294967295	0
user	Username for the Web resource.	string	Maximum length: 64	
password	Password for the Web resource.	password	Not Specified	
user-agent <name>	User agents can be used by this prefetch. User agent.	string	Maximum length: 79	

config webcache reverse-cache-server

Configure reverse cache server.

```

config webcache reverse-cache-server
  Description: Configure reverse cache server.
  edit <name>
    set ip {ipv4-address-any}
    set port {integer}
    set status [enable|disable]
    set priority {integer}
  next
end

```

config webcache reverse-cache-server

Parameter	Description	Type	Size	Default
name	Name of the reverse cache server	string	Maximum length: 35	
ip	Server IP address.	ipv4-address-any	Not Specified	0.0.0.0
port	Server port.	integer	Minimum value: 1 Maximum value: 65535	80
status	Enable/disable the cache server.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable the reverse-cache-server.	
		<i>disable</i>	Disable the reverse-cache-server.	
priority	Priority of the cache server (reserved).	integer	Minimum value: 0 Maximum value: 15	0

config webcache settings

Configure global Web cache settings.

```
config webcache settings
  Description: Configure global Web cache settings.
  set max-object-size {integer}
  set neg-resp-time {integer}
  set fresh-factor {integer}
  set max-ttl {integer}
  set min-ttl {integer}
  set default-ttl {integer}
  set ignore-ims [enable|disable]
  set ignore-conditional [enable|disable]
  set ignore-pnc [enable|disable]
  set ignore-ie-reload [enable|disable]
  set cache-expired [enable|disable]
  set cache-cookie [enable|disable]
  set reval-pnc [enable|disable]
  set always-revalidate [enable|disable]
  set cache-by-default [enable|disable]
```

```

set host-validate [enable|disable]
set add-x-cache [enable|disable]
set x-cache-message {string}
set external [enable|disable]
set crawler-user-agent {string}
end

```

config webcache settings

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
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
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
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
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: 1 Maximum value: 5256000	1440
ignore-ims	Enable/disable ignoring the if-modified-since (IMS) header.	option	-	disable

Parameter	Description	Type	Size	Default
	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-conditional	Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.	option	-	disable
	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-pnc	Enable/disable ignoring the pragma no-cache (PNC) header.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.		
	<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.		
ignore-ie-reload	Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.		
	<i>disable</i>	Disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.		
cache-expired	Enable/disable caching type-1 objects that are already expired on arrival.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable caching type-1 objects that have expired.		
	<i>disable</i>	Disable caching type-1 objects that have expired.		
cache-cookie	Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Cache cookies.		
	<i>disable</i>	Do not cache cookies.		
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).		
always-revalidate	Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.	option	-	disable
	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
	Option	Description		
	<i>enable</i>	Enable caching content that lacks explicit caching policies.		
	<i>disable</i>	Disable caching content that lacks explicit caching policies.		
host-validate	Enable/disable validating "Host:" with original server IP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable validating "Host:" with original server IP.		
	<i>disable</i>	Disable validating "Host:" with original server IP.		
add-x-cache	Enable/disable appending local "X-Cache: HIT/MISS" information when http-request is cacheable.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
x-cache-message	Config customized x-cache header message (use empty string to set to default).	string	Maximum length: 400	
external	Enable/disable external Web caching.	option	-	disable
	Option	Description		
	enable	Enable external Web caching		
	disable	Disable external Web caching		
crawler-user-agent	The user agent that the web crawler will use.	string	Maximum length: 255	fpx

config webcache user-agent

Configure reverse cache user agent.

```
config webcache user-agent
    Description: Configure reverse cache user agent.
    edit <name>
        set value {string}
    next
end
```

config webcache user-agent

Parameter	Description	Type	Size	Default
name	Name of the user agent item.	string	Maximum length: 35	
value	User agent of the URL.	string	Maximum length: 255	

webfilter

This section includes syntax for the following commands:

- [config webfilter categories on page 1403](#)
- [config webfilter content-header on page 1405](#)
- [config webfilter content on page 1403](#)
- [config webfilter domain-list on page 1406](#)
- [config webfilter fortiguard on page 1407](#)
- [config webfilter ftgd-local-cat on page 1410](#)
- [config webfilter ftgd-local-rating on page 1410](#)
- [config webfilter ftgd-local-risk on page 1411](#)
- [config webfilter ftgd-risk-level on page 1412](#)
- [config webfilter ftgd-statistics on page 1413](#)
- [config webfilter ips-urlfilter-cache-setting on page 1413](#)
- [config webfilter ips-urlfilter-setting on page 1413](#)
- [config webfilter ips-urlfilter-setting6 on page 1414](#)
- [config webfilter override-usr on page 1416](#)
- [config webfilter override on page 1415](#)
- [config webfilter profile on page 1417](#)
- [config webfilter search-engine on page 1435](#)
- [config webfilter status on page 1436](#)
- [config webfilter url-list on page 1440](#)
- [config webfilter urlfilter on page 1436](#)

config webfilter categories

List the FortiGuard Web Filter category descriptions.

```
config webfilter categories
    Description: List the FortiGuard Web Filter category descriptions.
end
```

config webfilter content

Configure Web filter banned word table.

```
config webfilter content
    Description: Configure Web filter banned word table.
```

```

edit <id>
    set name {string}
    set comment {var-string}
    config entries
        Description: Configure banned word entries.
        edit <name>
            set pattern-type [wildcard|regexp]
            set status [enable|disable]
            set lang [western|simch|...]
            set score {integer}
            set action [block|exempt]
        next
    end
next
end

```

config webfilter content

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

config entries

Parameter	Description	Type	Size	Default
name	Banned word.	string	Maximum length: 127	
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard
	Option	Description		
	wildcard	Wildcard pattern.		
	regex	Perl regular expression.		
status	Enable/disable banned word.	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.																							
lang	Language of banned word.	option	-	western																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>western</i></td><td>Western.</td></tr><tr><td><i>simch</i></td><td>Simplified Chinese.</td></tr><tr><td><i>trach</i></td><td>Traditional Chinese.</td></tr><tr><td><i>japanese</i></td><td>Japanese.</td></tr><tr><td><i>korean</i></td><td>Korean.</td></tr><tr><td><i>french</i></td><td>French.</td></tr><tr><td><i>thai</i></td><td>Thai.</td></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr><tr><td><i>cyrillic</i></td><td>Cyrillic.</td></tr></table>	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.			
	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.																							
score	Score, to be applied every time the word appears on a web page (0 - 4294967295, default = 10).	integer	Minimum value: 0 Maximum value: 4294967295	10																				
action	Block or exempt word when a match is found.	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>exempt</i></td><td>Exempt matches.</td></tr></table>	Option	Description	<i>block</i>	Block matches.	<i>exempt</i>	Exempt matches.																	
	Option	Description																						
	<i>block</i>	Block matches.																						
<i>exempt</i>	Exempt matches.																							

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 name {string}
    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
next
end

```

config webfilter content-header

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

config entries

Parameter	Description	Type	Size	Default
pattern	Content type (regular expression).	string	Maximum length: 31	
action	Action to take for this content type.	option	-	allow
	Option	Description		
	<i>block</i>	Block content type.		
	<i>allow</i>	Allow content type.		
	<i>exempt</i>	Exempt content type.		
category	Categories that this content type applies to.	user	Not Specified	all

config webfilter domain-list

Configure Web filter Domain list.

```

config webfilter domain-list
    Description: Configure Web filter Domain list.
    edit <name>
        set uuid {uuid}
        set status [enable|disable]
        set comment {var-string}
        config entries
            Description: Domain list entries.
            edit <domain>
                next
            end
        next
    end
end

```

config webfilter domain-list

Parameter	Description	Type	Size	Default						
name	Domain list name.	string	Maximum length: 35							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
status	Enable/disable Domain list.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Domain list.</td></tr><tr><td><i>disable</i></td><td>Disable Domain list.</td></tr></table>				Option	Description	<i>enable</i>	Enable Domain list.	<i>disable</i>	Disable Domain list.
	Option	Description								
	<i>enable</i>	Enable Domain list.								
<i>disable</i>	Disable Domain list.									
comment	Comment.	var-string	Maximum length: 255							

config entries

Parameter	Description	Type	Size	Default
domain	Domain.	string	Maximum length: 511	

config webfilter fortiguard

Configure FortiGuard Web Filter service.

```

config webfilter fortiguard
    Description: Configure FortiGuard Web Filter service.

```

```

set cache-mode [ttl|db-ver]
set cache-prefix-match [enable|disable]
set cache-mem-permille {integer}
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 ovr-auth-https [enable|disable]
set warn-auth-https [enable|disable]
set close-ports [enable|disable]
set request-packet-size-limit {integer}
set embed-image [enable|disable]
end

```

config webfilter fortiguard

Parameter	Description	Type	Size	Default
cache-mode	Cache entry expiration mode.	option	-	ttl
	Option		Description	
	<i>ttl</i>		Expire cache items by time-to-live.	
	<i>db-ver</i>		Expire cache items when the server DB version changes.	
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
cache-mem-permille	Maximum permille of available memory allocated to caching (1 - 150).	integer	Minimum value: 1 Maximum value: 150	1
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication.	integer	Minimum value: 0 Maximum value: 65535	8008

Parameter	Description	Type	Size	Default						
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						
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	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.									
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	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.									
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><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.									
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						

Parameter	Description	Type	Size	Default
embed-image	Enable/disable embedding images into replacement messages (default = enable).	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 status [enable|disable]
        set id {integer}
    next
end
```

config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default
status	Enable/disable the local category.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the local category.		
	<i>disable</i>	Disable the local category.		
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0
desc	Local category description.	string	Maximum length: 79	

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 status [enable|disable]
    set comment {var-string}
    set rating {user}
  next
end

```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default						
url	URL to rate locally.	string	Maximum length: 511							
status	Enable/disable local rating.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local rating.</td></tr><tr><td><i>disable</i></td><td>Disable local rating.</td></tr></table>				Option	Description	<i>enable</i>	Enable local rating.	<i>disable</i>	Disable local rating.
	Option	Description								
	<i>enable</i>	Enable local rating.								
<i>disable</i>	Disable local rating.									
comment	Comment.	var-string	Maximum length: 255							
rating	Local rating.	user	Not Specified							

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 status [enable|disable]
    set comment {var-string}
    set risk-score {integer}
  next
end

```

config webfilter ftgd-local-risk

Parameter	Description	Type	Size	Default
url	URL to rate locally.	string	Maximum length: 511	
status	Enable/disable local risk score.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local risk level.		
	<i>disable</i>	Disable local risk level.		
comment	Comment.	var-string	Maximum length: 255	
risk-score	Local risk score.	integer	Minimum value: 0 Maximum value: 100	0

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
name	Risk level name.	string	Maximum length: 35	
high	Risk level high.	integer	Minimum value: 0 Maximum value: 100	0

Parameter	Description	Type	Size	Default
low	Risk level low.	integer	Minimum value: 0 Maximum value: 100	0

config webfilter ftgd-statistics

Display rating cache and daemon statistics.

```
config webfilter ftgd-statistics
    Description: Display rating cache and daemon statistics.
end
```

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	

Parameter	Description	Type	Size	Default
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 status [enable|disable]
    set scope [user|user-group|...]
    set ip {ipv4-address}
    set user {string}
    set user-group {string}
    set old-profile {string}
    set new-profile {string}
    set ip6 {ipv6-address}
    set expires {user}
    set initiator {string}
  next
end

```

config webfilter override

Parameter	Description	Type	Size	Default
id	Override rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable override rule.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable override rule.</td></tr><tr><td><i>disable</i></td><td>Disable override rule.</td></tr></table>	Option	Description	<i>enable</i>	Enable override rule.	<i>disable</i>	Disable override rule.							
	Option	Description												
	<i>enable</i>	Enable override rule.												
<i>disable</i>	Disable override rule.													
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-	user										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Override the specified user.</td></tr><tr><td><i>user-group</i></td><td>Override the specified user group.</td></tr><tr><td><i>ip</i></td><td>Override the specified IP address.</td></tr><tr><td><i>ip6</i></td><td>Override the specified IPv6 address.</td></tr></table>	Option	Description	<i>user</i>	Override the specified user.	<i>user-group</i>	Override the specified user group.	<i>ip</i>	Override the specified IP address.	<i>ip6</i>	Override the specified IPv6 address.			
	Option	Description												
	<i>user</i>	Override the specified user.												
	<i>user-group</i>	Override the specified user group.												
	<i>ip</i>	Override the specified IP address.												
<i>ip6</i>	Override the specified IPv6 address.													
ip	IPv4 address which the override applies.	ipv4-address	Not Specified	0.0.0.0										
user	Name of the user which the override applies.	string	Maximum length: 64											
user-group	Specify the user group for which the override applies.	string	Maximum length: 63											
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 35											
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 35											
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified	::										
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 12:00:00										
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64											

config webfilter override-usr

Display list of user overrides.

```
config webfilter override-usr
    Description: Display list of user overrides.
end
```

config webfilter profile

Configure Web filter profiles.

```
config webfilter profile
  Description: Configure Web filter profiles.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set options {option1}, {option2}, ...
    set https-replacemsg [enable|disable]
    set web-flow-log-encoding [utf-8|punycode]
    set ovr-d-perm {option1}, {option2}, ...
    set post-action [normal|block]
  config override
    Description: Web Filter override settings.
    set ovr-d-cookie [allow|deny]
    set ovr-d-scope [user|user-group|...]
    set profile-type [list|radius]
    set ovr-d-dur-mode [constant|ask]
    set ovr-d-dur {user}
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set ovr-d-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
  end
config web
  Description: Web content filtering settings.
  set bword-threshold {integer}
  set bword-table {integer}
  set urlfilter-table {integer}
  set content-header-list {integer}
  set blocklist [enable|disable]
  set allowlist {option1}, {option2}, ...
  set safe-search {option1}, {option2}, ...
  set youtube-restrict [none|strict|...]
  set qwant-restrict [none|strict|...]
  set vimeo-restrict {string}
  set log-search [enable|disable]
  set keyword-match <pattern1>, <pattern2>, ...
end
config ftgd-wf
  Description: FortiGuard Web Filter settings.
  set options {option1}, {option2}, ...
  set exempt-quota {user}
  set ovr-d {user}
  config filters
    Description: FortiGuard filters.
    edit <id>
      set category {integer}
      set action [block|authenticate|...]
      set warn-duration {user}
```

```

        set auth-usr-grp <name1>, <name2>, ...
        set log [enable|disable]
        set override-replacemsg {string}
        set warning-prompt [per-domain|per-category]
        set warning-duration-type [session|timeout]
    next
end
config risk
    Description: FortiGuard risk level settings.
    edit <id>
        set risk-level {string}
        set action [block|monitor]
        set log [enable|disable]
    next
end
config quota
    Description: FortiGuard traffic quota settings.
    edit <id>
        set category {user}
        set type [time|traffic]
        set unit [B|KB|...]
        set value {integer}
        set duration {user}
        set override-replacemsg {string}
    next
end
set max-quota-timeout {integer}
set rate-javascript-urls [disable|enable]
set rate-css-urls [disable|enable]
set rate-crl-urls [disable|enable]
end
config antiphish
    Description: AntiPhishing profile.
    set status [enable|disable]
    set default-action [exempt|log|...]
    set check-uri [enable|disable]
    set check-basic-auth [enable|disable]
    set check-username-only [enable|disable]
    set max-body-len {integer}
    config inspection-entries
        Description: AntiPhishing entries.
        edit <name>
            set fortiguard-category {user}
            set action [exempt|log|...]
        next
    end
    config custom-patterns
        Description: Custom username and password regex patterns.
        edit <pattern>
            set category [username|password]
            set type [regex|literal]
        next
    end
end

```

```

        end
        set authentication [domain-controller|ldap]
        set domain-controller {string}
        set ldap {string}
    end
    set wisp [enable|disable]
    set wisp-servers <name1>, <name2>, ...
    set wisp-algorithm [primary-secondary|round-robin|...]
    set ia-categorization [enable|disable]
    set log-all-url [enable|disable]
    set web-content-log [enable|disable]
    set web-filter-activex-log [enable|disable]
    set web-filter-command-block-log [enable|disable]
    set web-filter-cookie-log [enable|disable]
    set web-filter-applet-log [enable|disable]
    set web-filter-jscript-log [enable|disable]
    set web-filter-js-log [enable|disable]
    set web-filter-vbs-log [enable|disable]
    set web-filter-unknown-log [enable|disable]
    set web-filter-referer-log [enable|disable]
    set web-filter-cookie-removal-log [enable|disable]
    set web-url-log [enable|disable]
    set web-invalid-domain-log [enable|disable]
    set web-ftgd-err-log [enable|disable]
    set web-ftgd-quota-usage [enable|disable]
    set web-antiphishing-log [enable|disable]
next
end

```

config webfilter profile

Parameter	Description	Type	Size	Default								
name	Profile name.	string	Maximum length: 35									
comment	Optional comments.	var-string	Maximum length: 255									
replacemsg-group	Replacement message group.	string	Maximum length: 35									
options	Options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>activexfilter</i></td><td>ActiveX filter.</td></tr><tr><td><i>cookiefilter</i></td><td>Cookie filter.</td></tr><tr><td><i>javafilter</i></td><td>Java applet filter.</td></tr></table>				Option	Description	<i>activexfilter</i>	ActiveX filter.	<i>cookiefilter</i>	Cookie filter.	<i>javafilter</i>	Java applet filter.
	Option	Description										
	<i>activexfilter</i>	ActiveX filter.										
	<i>cookiefilter</i>	Cookie filter.										
<i>javafilter</i>	Java applet filter.											

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block-invalid-url</i></td><td>Block sessions contained an invalid domain name.</td></tr><tr><td><i>jscript</i></td><td>Javascript block.</td></tr><tr><td><i>js</i></td><td>JS block.</td></tr><tr><td><i>vbs</i></td><td>VB script block.</td></tr><tr><td><i>unknown</i></td><td>Unknown script block.</td></tr><tr><td><i>intrinsic</i></td><td>Intrinsic script block.</td></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>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.	<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>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.																						
	<i>wf-referer</i>	Referring block.																						
	<i>wf-cookie</i>	Cookie block.																						
<i>per-user-bal</i>	Per-user block/allow list filter																							
https-replacemsg	Enable replacement messages for HTTPS.	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.																							
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																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>normal</i>	Normal, POST requests are allowed.		
	<i>block</i>	POST requests are blocked.		
wisp	Enable/disable web proxy WISP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable web proxy WISP.		
	<i>disable</i>	Disable web proxy WISP.		
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79	
wisp-algorithm	WISP server selection algorithm.	option	-	auto- learning
	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.		
ia- categorization	Enable/Disable use of image-analyzer engine to help categorize images with unknown category.	option	-	disable
	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.		
web-content- log	Enable/disable logging logging blocked web content.	option	-	enable

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-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-applet-log	Enable/disable logging Java applets.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-jscript-log	Enable/disable logging JScripts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-js-log	Enable/disable logging Java scripts.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-referer-log	Enable/disable logging referrers.	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.		
web-url-log	Enable/disable logging URL filtering.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-antiphishing-log	Enable/disable logging of AntiPhishing checks.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config override

Parameter	Description	Type	Size	Default
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow browser-based (cookie) override.		
	<i>deny</i>	Deny browser-based (cookie) override.		
ovrd-scope	Override scope.	option	-	user
	Option	Description		
	<i>user</i>	Override for the user.		

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></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-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-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.																			
profile-type	Override profile type.	option	-	list																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>list</i></td><td>Profile chosen from list.</td></tr><tr><td><i>radius</i></td><td>Profile determined by RADIUS server.</td></tr></table>	Option	Description	<i>list</i>	Profile chosen from list.	<i>radius</i>	Profile determined by RADIUS server.													
	Option	Description																		
	<i>list</i>	Profile chosen from list.																		
<i>radius</i>	Profile determined by RADIUS server.																			
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-dur	Override duration.	user	Not Specified	15m																
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><tr><td><i>Framed-IP-Address</i></td><td>Use this attribute.</td></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></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.	<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.			
	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.																			

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></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>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>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.																																			
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																																	

config web

Parameter	Description	Type	Size	Default										
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10										
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0										
blocklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blocklist.	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.													
allowlist	FortiGuard allowlist settings.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>exempt-av</td><td>Exempt antivirus.</td></tr><tr><td>exempt-webcontent</td><td>Exempt web content.</td></tr><tr><td>exempt-activex-java-cookie</td><td>Exempt ActiveX-JAVA-Cookie.</td></tr><tr><td>exempt-dlp</td><td>Exempt DLP.</td></tr></table>				Option	Description	exempt-av	Exempt antivirus.	exempt-webcontent	Exempt web content.	exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.	exempt-dlp	Exempt DLP.
Option	Description													
exempt-av	Exempt antivirus.													
exempt-webcontent	Exempt web content.													
exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.													
exempt-dlp	Exempt DLP.													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>exempt-rangeblock</i>	Exempt RangeBlock.		
	<i>extended-log-others</i>	Support extended log.		
safe-search	Safe search type.	option	-	
	Option	Description		
	<i>url</i>	Insert safe search string into URL.		
	<i>header</i>	Insert safe search header.		
youtube-restrict	YouTube EDU filter level.	option	-	none
	Option	Description		
	<i>none</i>	Full access for YouTube.		
	<i>strict</i>	Strict access for YouTube.		
	<i>moderate</i>	Moderate access for YouTube.		
qwant-restrict	Qwant safe search level.	option	-	strict
	Option	Description		
	<i>none</i>	Full access for Qwant.		
	<i>strict</i>	Strict access for Qwant.		
	<i>moderate</i>	Moderate access for Qwant.		
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	
log-search	Enable/disable logging all search phrases.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79	

config ftgd-wf

Parameter	Description	Type	Size	Default										
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error-allow</i></td><td>Allow web pages with a rating error to pass through.</td></tr><tr><td><i>rate-server-ip</i></td><td>Rate the server IP in addition to the domain name.</td></tr><tr><td><i>connect-request-bypass</i></td><td>Bypass connection which has CONNECT request.</td></tr><tr><td><i>ftgd-disable</i></td><td>Disable FortiGuard scanning.</td></tr></table>	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.			
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.													
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17										
ovrd	Allow web filter profile overrides.	user	Not Specified											
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300										
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rating JavaScript by URL.</td></tr><tr><td><i>enable</i></td><td>Enable rating JavaScript by URL.</td></tr></table>	Option	Description	<i>disable</i>	Disable rating JavaScript by URL.	<i>enable</i>	Enable rating JavaScript by URL.							
Option	Description													
<i>disable</i>	Disable rating JavaScript by URL.													
<i>enable</i>	Enable rating JavaScript by URL.													
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rating CSS by URL.</td></tr><tr><td><i>enable</i></td><td>Enable rating CSS by URL.</td></tr></table>	Option	Description	<i>disable</i>	Disable rating CSS by URL.	<i>enable</i>	Enable rating CSS by URL.							
Option	Description													
<i>disable</i>	Disable rating CSS by URL.													
<i>enable</i>	Enable rating CSS by URL.													
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rating CRL by URL.</td></tr><tr><td><i>enable</i></td><td>Enable rating CRL by URL.</td></tr></table>	Option	Description	<i>disable</i>	Disable rating CRL by URL.	<i>enable</i>	Enable rating CRL by URL.							
Option	Description													
<i>disable</i>	Disable rating CRL by URL.													
<i>enable</i>	Enable rating CRL by URL.													

config filters

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0
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.		
warn-duration	Duration of warnings.	user	Not Specified	5m
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79	
log	Enable/disable logging.	option	-	enable
	Option		Description	
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-replacemsg	Override replacement message.	string	Maximum length: 28	
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.		
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>session</i>	After session ends.		
	<i>timeout</i>	After timeout occurs.		

config risk

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
risk-level	Risk level to be examined.	string	Maximum length: 35	
action	Action to take for matches.	option	-	monitor
	Option	Description		
	<i>block</i>	Block access.		
	<i>monitor</i>	Allow access while logging the action.		
log	Enable/disable logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config quota

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
type	Quota type.	option	-	time

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>time</i>	Use a time-based quota.		
	<i>traffic</i>	Use a traffic-based quota.		
unit	Traffic quota unit of measurement.	option	-	MB
	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: 1 Maximum value: 4294967295	1024
duration	Duration of quota.	user	Not Specified	5m
override-replacemsg	Override replacement message.	string	Maximum length: 28	

config antiphish

Parameter	Description	Type	Size	Default
status	Toggle AntiPhishing functionality.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable AntiPhishing functionality.		
	<i>disable</i>	Disable AntiPhishing functionality.		
default-action	Action to be taken when there is no matching rule.	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.		

Parameter	Description	Type	Size	Default						
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-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-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.									
max-body-len	Maximum size of a POST body to check for credentials.	integer	Minimum value: 0 Maximum value: 4294967295	1024						
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.									
domain-controller	Domain for which to verify received credentials against.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default
ldap	LDAP server for which to verify received credentials against.	string	Maximum length: 63	

config inspection-entries

Parameter	Description	Type	Size	Default								
name	Inspection target name.	string	Maximum length: 63									
fortiguard-category	FortiGuard category to match.	user	Not Specified	0								
action	Action to be taken upon an AntiPhishing match.	option	-	exempt								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt requests from matching.</td></tr><tr><td><i>log</i></td><td>Log all matched requests.</td></tr><tr><td><i>block</i></td><td>Block all matched requests.</td></tr></table>				Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.
Option	Description											
<i>exempt</i>	Exempt requests from matching.											
<i>log</i>	Log all matched requests.											
<i>block</i>	Block all matched requests.											

config custom-patterns

Parameter	Description	Type	Size	Default						
pattern	Target pattern.	string	Maximum length: 255							
category	Category that the pattern matches.	option	-	username						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>username</i></td><td>Pattern matches username fields.</td></tr><tr><td><i>password</i></td><td>Pattern matches password fields.</td></tr></table>				Option	Description	<i>username</i>	Pattern matches username fields.	<i>password</i>	Pattern matches password fields.
	Option	Description								
	<i>username</i>	Pattern matches username fields.								
<i>password</i>	Pattern matches password fields.									
type	Pattern will be treated either as a regex pattern or literal string.	option	-	regex						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regex</i></td><td>Pattern will be treated as a regex pattern.</td></tr><tr><td><i>literal</i></td><td>Pattern will be treated as a literal string.</td></tr></table>				Option	Description	<i>regex</i>	Pattern will be treated as a regex pattern.	<i>literal</i>	Pattern will be treated as a literal string.
	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 webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
  Description: Configure web filter search engines.
  edit <name>
    set hostname {string}
    set url {string}
    set query {string}
    set safesearch [disable|url|...]
    set charset [utf-8|gb2312]
    set source-url [enable|disable]
    set safesearch-str {string}
  next
end
```

config webfilter search-engine

Parameter	Description	Type	Size	Default
name	Search engine name.	string	Maximum length: 35	
hostname	Hostname (regular expression).	string	Maximum length: 127	
url	URL (regular expression).	string	Maximum length: 127	
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
		Option	Description	
		<i>disable</i>	Site does not support safe search.	
		<i>url</i>	Safe search selected with a parameter in the URL.	
		<i>header</i>	Safe search selected by search header (i.e. youtube.edu).	
		<i>translate</i>	Perform URL FortiGuard check on translated URL.	
		<i>yt-pattern</i>	Pattern to match YouTube channel ID.	
		<i>yt-scan</i>	Perform IPS scan.	
		<i>yt-video</i>	Pattern to match YouTube video name.	

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yt-channel</i></td><td>Pattern to match YouTube channel name.</td></tr></table>	Option	Description	<i>yt-channel</i>	Pattern to match YouTube channel name.					
Option	Description									
<i>yt-channel</i>	Pattern to match YouTube channel name.									
charset	Search engine charset.	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>gb2312</i></td><td>GB2312 encoding.</td></tr></table>	Option	Description	<i>utf-8</i>	UTF-8 encoding.	<i>gb2312</i>	GB2312 encoding.			
Option	Description									
<i>utf-8</i>	UTF-8 encoding.									
<i>gb2312</i>	GB2312 encoding.									
source-url	Enable/disable source url in the image search result.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source url in image search.</td></tr><tr><td><i>disable</i></td><td>Disable source url in image search.</td></tr></table>	Option	Description	<i>enable</i>	Enable source url in image search.	<i>disable</i>	Disable source url in image search.			
Option	Description									
<i>enable</i>	Enable source url in image search.									
<i>disable</i>	Disable source url in image search.									
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							

config webfilter status

Display rating info.

```
config webfilter status
    Description: Display rating info.
    set <refresh-rate> {string}
end
```

config webfilter status

Parameter	Description	Type	Size	Default
<refresh-rate>	Frequency to refresh the server list (sec).	string	Maximum length: -	

config webfilter urlfilter

Configure URL filter lists.


```

config webfilter urlfilter
    Description: Configure URL filter lists.
    edit <id>
        set name {string}
        set comment {var-string}
        set one-arm-ips-urlfilter [enable|disable]
        set ip-addr-block [enable|disable]
        set ip4-mapped-ip6 [enable|disable]
        set include-subdomains [enable|disable]
    config entries
        Description: URL filter entries.
        edit <id>
            set url {string}
            set type [simple|regex|...]
            set action [exempt|block|...]
            set antiphish-action [block|log]
            set status [enable|disable]
            set exempt {option1}, {option2}, ...
            set web-proxy-profile {string}
            set referrer-host {string}
            set dns-address-family [ipv4|ipv6|...]
        next
    end
next
end

```

config webfilter urlfilter

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of URL filter list.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.	
		<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.	

Parameter	Description	Type	Size	Default						
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><i>enable</i></td><td>Enable blocking URLs when the hostname appears as an IP address.</td></tr><tr><td><i>disable</i></td><td>Disable blocking URLs when the hostname appears as an IP address.</td></tr></table>	Option	Description	<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.	<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.			
Option	Description									
<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.									
<i>disable</i>	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><i>enable</i></td><td>Enable matching IPv4 mapped IPv6 URLs.</td></tr><tr><td><i>disable</i></td><td>Disable matching IPv4 mapped IPv6 URLs.</td></tr></table>	Option	Description	<i>enable</i>	Enable matching IPv4 mapped IPv6 URLs.	<i>disable</i>	Disable matching IPv4 mapped IPv6 URLs.			
Option	Description									
<i>enable</i>	Enable matching IPv4 mapped IPv6 URLs.									
<i>disable</i>	Disable matching IPv4 mapped IPv6 URLs.									
include-subdomains	Enable/disable matching subdomains, only applies to simple type (default: enable).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable matching subdomains, only applies to simple type.</td></tr><tr><td><i>disable</i></td><td>Disable matching subdomains, only applies to simple type.</td></tr></table>	Option	Description	<i>enable</i>	Enable matching subdomains, only applies to simple type.	<i>disable</i>	Disable matching subdomains, only applies to simple type.			
Option	Description									
<i>enable</i>	Enable matching subdomains, only applies to simple type.									
<i>disable</i>	Disable matching subdomains, only applies to simple type.									

config entries

Parameter	Description	Type	Size	Default								
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0								
url	URL to be filtered.	string	Maximum length: 511									
type	Filter type (simple, regex, or wildcard).	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple URL string.</td></tr><tr><td><i>regex</i></td><td>Regular expression URL string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard URL string.</td></tr></table>				Option	Description	<i>simple</i>	Simple URL string.	<i>regex</i>	Regular expression URL string.	<i>wildcard</i>	Wildcard URL string.
Option	Description											
<i>simple</i>	Simple URL string.											
<i>regex</i>	Regular expression URL string.											
<i>wildcard</i>	Wildcard URL string.											

Parameter	Description	Type	Size	Default
action	Action to take for URL filter matches.	option	-	exempt
	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
	Option	Description		
	<i>block</i>	Block matches.		
	<i>log</i>	Allow matches with log.		
status	Enable/disable this URL filter.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this URL filter.		
	<i>disable</i>	Disable this URL filter.		
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
	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.		
web-proxy-profile	Web proxy profile.	string	Maximum length: 63	
referrer-host	Referrer host name.	string	Maximum length: 255	
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4
	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.		

config webfilter url-list

Configure Web filter URL list.

```

config webfilter url-list
  Description: Configure Web filter URL list.
  edit <name>
    set uuid {uuid}
    set status [enable|disable]
    set comment {var-string}
    config entries
      Description: URL list entries.
      edit <url>
        next
      end
    end
  next
end

```

config webfilter url-list

Parameter	Description	Type	Size	Default
name	URL list name.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
status	Enable/disable URL list.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable URL list.		
	<i>disable</i>	Disable URL list.		
comment	Comment.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
url	URL.	string	Maximum length: 511	

ztna

This section includes syntax for the following commands:

- [config ztna connector-service-edge on page 1442](#)
- [config ztna reverse-connector on page 1443](#)
- [config ztna service-connector on page 1444](#)
- [config ztna traffic-forward-proxy on page 1447](#)
- [config ztna web-portal-bookmark on page 1453](#)
- [config ztna web-portal on page 1448](#)
- [config ztna web-proxy on page 1459](#)

config ztna connector-service-edge

Configure ZTNA connector service edge.

```
config ztna connector-service-edge
  Description: Configure ZTNA connector service edge.
  set status [enable|disable]
  set interface <name1>, <name2>, ...
  set port {integer}
  set ssl-max-version [tls-1.1|tls-1.2|...]
  set server-cert {string}
  set trusted-client-ca <name1>, <name2>, ...
end
```

config ztna connector-service-edge

Parameter	Description	Type	Size	Default
status	Connector service edge status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the connector service edge.		
	<i>disable</i>	Disable the connector service edge.		
interface <name>	Connector service edge interface. Interface name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default								
port	Connector service edge port(1-65535, default 8443).	integer	Minimum value: 1 Maximum value: 65535	8443								
ssl-max-version	Highest TLS version accepted by 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.											
server-cert	Server certificate for mTLS.	string	Maximum length: 79	Fortinet_SSL								
trusted-client-ca <name>	CA certificate used for client certificate verification. CA certificate list.	string	Maximum length: 79									

config ztna reverse-connector

Configure ZTNA Reverse-Connector.

```

config ztna reverse-connector
  Description: Configure ZTNA Reverse-Connector.
  edit <name>
    set status [enable|disable]
    set address {string}
    set port {integer}
    set health-check-interval {integer}
    set ssl-max-version [tls-1.1|tls-1.2|...]
    set certificate {string}
    set trusted-server-ca {string}
  next
end

```

config ztna reverse-connector

Parameter	Description	Type	Size	Default
name	Reverse connector name	string	Maximum length: 35	

Parameter	Description	Type	Size	Default								
status	Reverse connector status.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the server.</td></tr><tr><td><i>disable</i></td><td>Disable the server.</td></tr></table>				Option	Description	<i>enable</i>	Enable the server.	<i>disable</i>	Disable the server.		
	Option	Description										
	<i>enable</i>	Enable the server.										
<i>disable</i>	Disable the server.											
address	Reverse connector adress(IP or FQDN).	string	Maximum length: 255									
port	Port number that traffic uses to connect to remote server (0 - 65535;).	integer	Minimum value: 0 Maximum value: 65535	0								
health-check-interval	Health check interval in seconds (0 - 600, default = 60, 0 = disable).	integer	Minimum value: 0 Maximum value: 600	60								
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><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-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.
	Option	Description										
	<i>tls-1.1</i>	TLS 1.1.										
	<i>tls-1.2</i>	TLS 1.2.										
<i>tls-1.3</i>	TLS 1.3.											
certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35									
trusted-server-ca	Trusted Server CA certificate used by SSL connection.	string	Maximum length: 79									

config ztna service-connector

Configure ZTNA service connector.

```
config ztna service-connector
  Description: Configure ZTNA service connector.
  edit <name>
    set status [enable|disable]
    set connection-mode [forward|reverse]
    set forward-address {string}
    set forward-port {integer}
    set forward-destination-cn {string}
```



```

set certificate {string}
set trusted-ca {string}
set encryption [enable|disable]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set url-map {string}
set relay-dev-info [enable|disable]
set relay-user-info [enable|disable]
set log [enable|disable]
set health-check-interval {integer}
next
end

```

config ztna service-connector

Parameter	Description	Type	Size	Default						
name	Service-connector name	string	Maximum length: 79							
status	Service-connector status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the service-connector.</td></tr><tr><td><i>disable</i></td><td>Disable the service-connector.</td></tr></table>				Option	Description	<i>enable</i>	Enable the service-connector.	<i>disable</i>	Disable the service-connector.
	Option	Description								
	<i>enable</i>	Enable the service-connector.								
<i>disable</i>	Disable the service-connector.									
connection-mode	Connection mode.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward Service.</td></tr><tr><td><i>reverse</i></td><td>Reverse Service.</td></tr></table>				Option	Description	<i>forward</i>	Forward Service.	<i>reverse</i>	Reverse Service.
	Option	Description								
	<i>forward</i>	Forward Service.								
<i>reverse</i>	Reverse Service.									
forward-address	service-connector address(IP or FQDN, reverse gateway must configure IP address).	string	Maximum length: 255							
forward-port	Port number that forward traffic uses to connect to	integer	Minimum value: 1 Maximum value: 65535	0						
forward-destination-cn	CN for forward server.	string	Maximum length: 255							
certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default												
trusted-ca	Trusted CA certificate used by SSL inspection.	string	Maximum length: 79													
encryption	Enable/disable Encryption (default = disable).	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Encryption.</td></tr><tr><td><i>disable</i></td><td>Disable Encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable Encryption.	<i>disable</i>	Disable Encryption.									
Option	Description															
<i>enable</i>	Enable Encryption.															
<i>disable</i>	Disable Encryption.															
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.2												
	<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 server.	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.															
url-map	URL pattern to match.	string	Maximum length: 63	/tcp												
relay-dev-info	Enable/disable device info relay.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Relay device information to service connector</td></tr><tr><td><i>disable</i></td><td>Do not relay device information to service connector.</td></tr></table>	Option	Description	<i>enable</i>	Relay device information to service connector	<i>disable</i>	Do not relay device information to service connector.									
Option	Description															
<i>enable</i>	Relay device information to service connector															
<i>disable</i>	Do not relay device information to service connector.															
relay-user-info	Enable/disable user info relay.	option	-	disable												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Relay user information to service connector		
	<i>disable</i>	Do not relay user information to service connector.		
log	Enable/disable logging of traffic.	option	-	enable
	Option	Description		
	<i>enable</i>	Log all traffic by this service connector.		
	<i>disable</i>	Do not log traffic by this service connector.		
health-check-interval	health check interval(0-600 seconds, default 60, 0 means disable).	integer	Minimum value: 0 Maximum value: 600	60

config ztna traffic-forward-proxy

Configure ZTNA traffic-forward-proxy.

```

config ztna traffic-forward-proxy
  Description: Configure ZTNA traffic-forward-proxy.
  edit <name>
    config url-route
      Description: Set URL Route.
      edit <name>
        set url-pattern {string}
        set service-connector {string}
      next
    end
    set vip {string}
    set host {string}
    set decrypted-traffic-mirror {string}
    set log-blocked-traffic [disable|enable]
    set auth-portal [disable|enable]
    set auth-virtual-host {string}
  next
end

```

config ztna traffic-forward-proxy

Parameter	Description	Type	Size	Default						
name	ZTNA proxy name.	string	Maximum length: 79							
vip	Virtual IP name.	string	Maximum length: 79							
host	Virtual or real host name.	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><i>disable</i></td><td>Do not log all traffic denied by this ZTNA web-proxy.</td></tr><tr><td><i>enable</i></td><td>Log all traffic denied by this ZTNA web-proxy.</td></tr></table>				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.
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.									
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication portal.</td></tr><tr><td><i>enable</i></td><td>Enable authentication portal.</td></tr></table>				Option	Description	<i>disable</i>	Disable authentication portal.	<i>enable</i>	Enable authentication portal.
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							

config url-route

Parameter	Description	Type	Size	Default
name	URL Route name	string	Maximum length: 79	
url-pattern	URL pattern to match.	string	Maximum length: 511	/tcp
service-connector	Service Connector.	string	Maximum length: 79	

config ztna web-portal

Configure ztna web-portal.

```

config ztna web-portal
  Description: Configure ztna web-portal.
  edit <name>
    set vip {string}
    set host {string}
    set decrypted-traffic-mirror {string}
    set log-blocked-traffic [disable|enable]
    set auth-portal [disable|enable]
    set auth-virtual-host {string}
    set auth-rule {string}
    set display-bookmark [enable|disable]
    set focus-bookmark [enable|disable]
    set display-status [enable|disable]
    set display-history [enable|disable]
    set policy-auth-sso [enable|disable]
    set heading {string}
    set theme [jade|neutrino|...]
    set clipboard [enable|disable]
    set default-window-width {integer}
    set default-window-height {integer}
    set cookie-age {integer}
    set forticlient-download [enable|disable]
    set forticlient-download-method [direct|ssl-vpn]
    set customize-forticlient-download-url [enable|disable]
    set windows-forticlient-download-url {var-string}
    set macos-forticlient-download-url {var-string}
    set bookmarks {string}
  next
end

```

config ztna web-portal

Parameter	Description	Type	Size	Default
name	ZTNA proxy name.	string	Maximum length: 79	
vip	Virtual IP name.	string	Maximum length: 79	
host	Virtual or real host name.	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

Parameter	Description	Type	Size	Default
	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.		
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	
auth-rule	Authentication Rule.	string	Maximum length: 35	
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
focus-bookmark	Enable to prioritize the placement of the bookmark section over the quick-connection section in the ztna web-portal.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
display-status	Enable to display the web portal status widget.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
display-history	Enable to display the web portal user login history widget.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
policy-auth- sso	Enable policy sso authentication.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
heading	Web portal heading message.	string	Maximum length: 31	ZTNA Portal
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.		
clipboard	Enable to support RDP/VPC clipboard functionality.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable support of RDP/VNC clipboard.		
	<i>disable</i>	Disable support of RDP/VNC clipboard.		

Parameter	Description	Type	Size	Default						
default-window-width	Screen width (range from 0 - 65535, default = 1024).	integer	Minimum value: 0 Maximum value: 65535	1024						
default-window-height	Screen height (range from 0 - 65535, default = 768).	integer	Minimum value: 0 Maximum value: 65535	768						
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						
forticlient-download	Enable/disable download option for FortiClient.	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.									
forticlient-download-method	FortiClient download method.	option	-	direct						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>direct</i></td><td>Download via direct link.</td></tr><tr><td><i>ssl-vpn</i></td><td>Download via SSL-VPN.</td></tr></table>				Option	Description	<i>direct</i>	Download via direct link.	<i>ssl-vpn</i>	Download via SSL-VPN.
Option	Description									
<i>direct</i>	Download via direct link.									
<i>ssl-vpn</i>	Download via SSL-VPN.									
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.									
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023							

Parameter	Description	Type	Size	Default
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023	
bookmarks	Dynamic bookmarks.	string	Maximum length: 35	

config ztna web-portal-bookmark

Configure ztna web-portal bookmark.

```

config ztna web-portal-bookmark
  Description: Configure ztna web-portal bookmark.
  edit <name>
    set type [user|ldap-dynamic|...]
    set users <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set apptype [ftp|rdp|...]
        set url {var-string}
        set host {var-string}
        set folder {var-string}
        set domain {var-string}
        set description {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set security [any|rdp|...]
        set send-preconnection-id [enable|disable]
        set preconnection-id {integer}
        set preconnection-blob {var-string}
        set load-balancing-info {var-string}
        set restricted-admin [enable|disable]
        set port {integer}
        set logon-user {var-string}
        set logon-password {password}
        set color-depth [32|16|...]
        set sso [disable|enable]
        set width {integer}
        set height {integer}
        set vnc-keyboard-layout [default|da|...]
      next
    end
  next
end

```

config ztna web-portal-bookmark

Parameter	Description	Type	Size	Default
name	Bookmark name.	string	Maximum length: 35	
type	Bookmark type	option	-	user
	Option	Description		
	<i>user</i>	Users/Groups.		
	<i>ldap-dynamic</i>	LDAP attributes dynamic.		
	<i>saml-dynamic</i>	SAML attributes dynamic.		
users <name>	User name. User name.	string	Maximum length: 79	
groups <name>	User groups. Group name.	string	Maximum length: 79	

config bookmarks

Parameter	Description	Type	Size	Default																		
name	Bookmark name.	string	Maximum length: 35																			
apptype	Application type.	option	-	web																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>rdp</i></td><td>RDP.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>smb</i></td><td>SMB/CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr><tr><td><i>telnet</i></td><td>Telnet.</td></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>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.	<i>web</i>	HTTP/HTTPS.			
	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.																				
<i>web</i>	HTTP/HTTPS.																					
url	URL parameter.	var-string	Maximum length: 128																			
host	Host name/IP parameter.	var-string	Maximum length: 128																			

Parameter	Description	Type	Size	Default																																																
folder	Network shared file folder parameter.	var-string	Maximum length: 128																																																	
domain	Login domain.	var-string	Maximum length: 128																																																	
description	Description.	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><tr><td><i>de-ch</i></td><td>German, Switzerland.</td></tr><tr><td><i>de-ibm</i></td><td>German (IBM).</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>en-us</i></td><td>English, United States.</td></tr><tr><td><i>en-us-dvorak</i></td><td>English, United States-Dvorak.</td></tr><tr><td><i>es</i></td><td>Spanish.</td></tr><tr><td><i>es-var</i></td><td>Spanish Variation.</td></tr><tr><td><i>fi</i></td><td>Finnish.</td></tr><tr><td><i>fi-sami</i></td><td>Finnish with Sami.</td></tr><tr><td><i>fr</i></td><td>French.</td></tr><tr><td><i>fr-apple</i></td><td>French, Apple.</td></tr><tr><td><i>fr-ca</i></td><td>French, Canada.</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.	<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.
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.																																																			
<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.																																																			

Parameter	Description	Type	Size	Default

Option	Description
<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).
<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.

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>sv-sami</i></td><td>Swedish with Sami.</td></tr><tr><td><i>tuk</i></td><td>Turkmen.</td></tr><tr><td><i>tur-f</i></td><td>Turkish F.</td></tr><tr><td><i>tur-q</i></td><td>Turkish Q.</td></tr><tr><td><i>zh-sym-sg-us</i></td><td>Chinese (Simplified, Singapore) - US keyboard.</td></tr><tr><td><i>zh-sym-us</i></td><td>Chinese (Simplified) - US Keyboard.</td></tr><tr><td><i>zh-tr-hk</i></td><td>Chinese (Traditional, Hong Kong S.A.R.).</td></tr><tr><td><i>zh-tr-mo</i></td><td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td></tr><tr><td><i>zh-tr-us</i></td><td>Chinese (Traditional) - US keyboard.</td></tr></table>	Option	Description	<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.			
	Option	Description																								
	<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.																									
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.																									
preconnection-id	The numeric ID of the RDP source (0-4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	0																						
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511																							

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									
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.											
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0								
logon-user	Logon user.	var-string	Maximum length: 35									
logon-password	Logon password.	password	Not Specified									
color-depth	Color depth per pixel.	option	-	16								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>32</i></td><td>32bits per pixel.</td></tr><tr><td><i>16</i></td><td>16bits per pixel.</td></tr><tr><td><i>8</i></td><td>8bits per pixel.</td></tr></table>				Option	Description	<i>32</i>	32bits per pixel.	<i>16</i>	16bits per pixel.	<i>8</i>	8bits per pixel.
	Option	Description										
	<i>32</i>	32bits per pixel.										
	<i>16</i>	16bits per pixel.										
<i>8</i>	8bits per pixel.											
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>enable</i></td><td>Enable SSO.</td></tr></table>				Option	Description	<i>disable</i>	Disable SSO.	<i>enable</i>	Enable SSO.		
	Option	Description										
	<i>disable</i>	Disable SSO.										
<i>enable</i>	Enable SSO.											
width	Screen width (range from 0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0								
height	Screen height (range from 0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535	0								
vnc-keyboard-layout	Keyboard layout.	option	-	default								

Parameter	Description	Type	Size	Default
	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.		
	<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.		

config ztna web-proxy

Configure ZTNA web-proxy.

```
config ztna web-proxy
  Description: Configure ZTNA web-proxy.
  edit <name>
    set vip {string}
    set host {string}
    set decrypted-traffic-mirror {string}
    set log-blocked-traffic [disable|enable]
    set auth-portal [disable|enable]
    set auth-virtual-host {string}
```

```

set vip6 {string}
set svr-pool-multiplex [enable|disable]
set svr-pool-ttl {integer}
set svr-pool-server-max-request {integer}
set svr-pool-server-max-concurrent-request {integer}
config api-gateway
    Description: Set IPv4 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https]
        set ldb-method [static|round-robin|...]
        set url-map-type [sub-string|wildcard|...]
        set h2-support [enable|disable]
        set h3-support [enable|disable]
    config quic
        Description: QUIC setting.
        set max-idle-timeout {integer}
        set max-udp-payload-size {integer}
        set active-connection-id-limit {integer}
        set ack-delay-exponent {integer}
        set max-ack-delay {integer}
        set max-datagram-frame-size {integer}
        set active-migration [enable|disable]
        set grease-quic-bit [enable|disable]
    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 ip {ipv4-address-any}
            set port {integer}
            set status [active|standby|...]
            set weight {integer}
            set http-host {string}
            set health-check [disable|enable]
            set health-check-proto [ping|http|...]
            set holddown-interval [enable|disable]
            set translate-host [enable|disable]
            set verify-cert [enable|disable]
        next
    end
    set persistence [none|http-cookie]
    set http-cookie-domain-from-host [disable|enable]
    set http-cookie-domain {string}
    set http-cookie-path {string}
    set http-cookie-generation {integer}
    set http-cookie-age {integer}
    set http-cookie-share [disable|same-ip]
    set https-cookie-secure [disable|enable]
    set ssl-dh-bits [768|1024|...]

```



```

        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-min-version [tls-1.0|tls-1.1|...]
        set ssl-max-version [tls-1.0|tls-1.1|...]
        set ssl-renegotiation [enable|disable]
    next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https]
        set ldb-method [static|round-robin|...]
        set url-map-type [sub-string|wildcard|...]
        set h2-support [enable|disable]
        set h3-support [enable|disable]
        config quic
            Description: QUIC setting.
            set max-idle-timeout {integer}
            set max-udp-payload-size {integer}
            set active-connection-id-limit {integer}
            set ack-delay-exponent {integer}
            set max-ack-delay {integer}
            set max-datagram-frame-size {integer}
            set active-migration [enable|disable]
            set grease-quic-bit [enable|disable]
        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 ip {ipv6-address}
                set port {integer}
                set status [active|standby|...]
                set weight {integer}
                set http-host {string}
                set health-check [disable|enable]
                set health-check-proto [ping|http|...]
                set holddown-interval [enable|disable]
                set translate-host [enable|disable]
                set verify-cert [enable|disable]
            next
        end
        set persistence [none|http-cookie]
    end
end

```

```

set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set ssl-dh-bits [768|1024|...]
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-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
next
end
next
end

```

config ztna web-proxy

Parameter	Description	Type	Size	Default						
name	ZTNA proxy name.	string	Maximum length: 79							
vip	Virtual IP name.	string	Maximum length: 79							
host	Virtual or real host name.	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><i>disable</i></td><td>Do not log all traffic denied by this ZTNA web-proxy.</td></tr><tr><td><i>enable</i></td><td>Log all traffic denied by this ZTNA web-proxy.</td></tr></table>				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.
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.									
auth-portal	Enable/disable authentication portal.	option	-	disable						

Parameter	Description	Type	Size	Default
	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	
vip6	Virtual IPv6 name.	string	Maximum length: 79	
svr-pool-multiplex	Enable/disable server pool multiplexing. Share connected server in HTTP and HTTPS api-gateways.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable server pool multiplexing. Share connected server.		
	<i>disable</i>	Disable server pool multiplexing. Do not share connected server.		
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15
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-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

config api-gateway

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

Parameter	Description	Type	Size	Default												
url-map	URL pattern to match.	string	Maximum length: 511	/												
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>https</td><td>HTTPS.</td></tr></table>				Option	Description	http	HTTP.	https	HTTPS.						
	Option	Description														
	http	HTTP.														
	https	HTTPS.														
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Distribute to servers based on source IP.</td></tr><tr><td>round-robin</td><td>Distribute to servers based on round-robin order.</td></tr><tr><td>weighted</td><td>Distribute to servers based on weight.</td></tr><tr><td>first-alive</td><td>Distribute to the first server that is alive.</td></tr><tr><td>http-host</td><td>Distribute to servers based on the host field in HTTP header.</td></tr></table>				Option	Description	static	Distribute to servers based on source IP.	round-robin	Distribute to servers based on round-robin order.	weighted	Distribute to servers based on weight.	first-alive	Distribute to the first server that is alive.	http-host	Distribute to servers based on the host field in HTTP header.
	Option	Description														
	static	Distribute to servers based on source IP.														
	round-robin	Distribute to servers based on round-robin order.														
	weighted	Distribute to servers based on weight.														
	first-alive	Distribute to the first server that is alive.														
http-host	Distribute to servers based on the host field in HTTP header.															
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.															
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.															

Parameter	Description	Type	Size	Default						
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.									
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><i>disable</i></td><td>Disable use of HTTP cookie domain from the host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from the host field in HTTP.</td></tr></table>	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.			
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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
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-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-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><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 the 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 the 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.																	
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-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-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.																	

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-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.													

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3

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						
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.									

config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
	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	

Parameter	Description	Type	Size	Default								
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>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.											
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								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
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 health check per server.</td></tr><tr><td>enable</td><td>Enable health check per server.</td></tr></table>				Option	Description	disable	Disable health check per server.	enable	Enable health check per server.		
Option	Description											
disable	Disable health check per server.											
enable	Enable health check per server.											
health-check-protocol	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.											

Parameter	Description	Type	Size	Default						
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.									
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.									
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.									

config ssl-cipher-suites

Parameter	Description	Type	Size	Default						
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0						
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></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.
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.									

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></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.			
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.																							

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></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></table>	Option	Description	<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.	<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.			
Option	Description																							
<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.																							
<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.																							

Parameter	Description	Type	Size	Default
	Option	Description		
	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.		
	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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></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-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.									
Option	Description													
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.													
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								
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
url-map	URL pattern to match.	string	Maximum length: 511	/								
service	Service.	option	-	https								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>https</td><td>HTTPS.</td></tr></table>				Option	Description	http	HTTP.	https	HTTPS.		
Option	Description											
http	HTTP.											
https	HTTPS.											
ldb-method	Method used to distribute sessions to real servers.	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Distribute to servers based on source IP.</td></tr><tr><td>round-robin</td><td>Distribute to servers based on round-robin order.</td></tr><tr><td>weighted</td><td>Distribute to servers based on weight.</td></tr></table>				Option	Description	static	Distribute to servers based on source IP.	round-robin	Distribute to servers based on round-robin order.	weighted	Distribute to servers based on weight.
Option	Description											
static	Distribute to servers based on source IP.											
round-robin	Distribute to servers based on round-robin order.											
weighted	Distribute to servers based on weight.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		
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.		
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.		
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).		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from the host field in HTTP.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of HTTP cookie domain from the host field in HTTP.					
Option	Description									
<i>enable</i>	Enable use of HTTP cookie domain from the host field in HTTP.									
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
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-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-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><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 the 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 the 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.									
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.									
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048						

Parameter	Description	Type	Size	Default														
	<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-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>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.																
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-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-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.		

config quic

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
active-connection-id-limit	Active connection ID limit (1 - 8, default = 2).	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent (1 - 20, default = 3).	integer	Minimum value: 1 Maximum value: 20	3
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
active-migration	Enable/disable active migration (default = disable).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable active migration.		
	<i>disable</i>	Disable active migration.		

Parameter	Description	Type	Size	Default
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.		

config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
	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	
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
	Option Description			
	<i>active</i>	Server status active.		
	<i>standby</i>	Server status standby.		
	<i>disable</i>	Server status disable.		

Parameter	Description	Type	Size	Default								
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								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
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 health check per server.</td></tr><tr><td>enable</td><td>Enable health check per server.</td></tr></table>				Option	Description	disable	Disable health check per server.	enable	Enable health check per server.		
Option	Description											
disable	Disable health check per server.											
enable	Enable health check per server.											
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								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable per server holddown.</td></tr><tr><td>disable</td><td>Disable per server holddown.</td></tr></table>				Option	Description	enable	Enable per server holddown.	disable	Disable per server holddown.		
Option	Description											
enable	Enable per server holddown.											
disable	Disable per server holddown.											
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.											
verify-cert	Enable/disable certificate verification of the real server.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable certificate verification.		
	<i>disable</i>	Disable certificate verification.		

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
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><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-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-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																				
	<table><tr><th>Option</th><th>Description</th></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><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.</td></tr></table>	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.			
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		
	<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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	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.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></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><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></table>	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.			
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.																					
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 1494](#)
- [diagnose antivirus on page 1495](#)
- [diagnose automation on page 1498](#)
- [diagnose autoupdate on page 1498](#)
- [diagnose casb on page 1499](#)
- [diagnose debug on page 1502](#)
- [diagnose disktest on page 1576](#)
- [diagnose emailfilter on page 1579](#)
- [diagnose endpoint on page 1580](#)
- [diagnose fdsm on page 1600](#)
- [diagnose firewall on page 1606](#)
- [diagnose fortiguard-resources on page 1624](#)
- [diagnose fortitoken-cloud on page 1639](#)
- [diagnose fortitoken on page 1638](#)
- [diagnose fortiview on page 1642](#)
- [diagnose geoip on page 1643](#)
- [diagnose hardware on page 1645](#)
- [diagnose http-view on page 1649](#)
- [diagnose ip on page 1650](#)
- [diagnose ip address on page 1655](#)
- [diagnose ip arp on page 1656](#)
- [diagnose ip parp on page 1657](#)
- [diagnose ip route on page 1657](#)
- [diagnose ip tcp on page 1659](#)
- [diagnose ip udp on page 1659](#)
- [diagnose ipsec on page 1659](#)
- [diagnose ipset on page 1661](#)
- [diagnose iptables on page 1661](#)
- [diagnose ipv6 on page 1662](#)
- [diagnose ipv6 address on page 1666](#)
- [diagnose ipv6 neighbor-cache on page 1667](#)
- [diagnose ipv6 route on page 1668](#)
- [diagnose lldprx on page 1668](#)
- [diagnose log on page 1672](#)
- [diagnose netlink on page 1676](#)

- [diagnose nodejs on page 1681](#)
- [diagnose oci on page 1684](#)
- [diagnose on-demand-sniffer on page 1684](#)
- [diagnose preload on page 1685](#)
- [diagnose report-runner-v2 on page 1689](#)
- [diagnose report-runner on page 1688](#)
- [diagnose report on page 1687](#)
- [diagnose saas on page 1690](#)
- [diagnose settings on page 1691](#)
- [diagnose sniffer on page 1692](#)
- [diagnose snmp on page 1695](#)
- [diagnose sys on page 1698](#)
- [diagnose test analytics-pdf-report on page 1799](#)
- [diagnose test analytics-report on page 1800](#)
- [diagnose test application on page 1801](#)
- [diagnose test authserver on page 1821](#)
- [diagnose test guest on page 1823](#)
- [diagnose test security on page 1824](#)
- [diagnose test update on page 1825](#)
- [diagnose tpm on page 1825](#)
- [diagnose traffictest on page 1827](#)
- [diagnose user-device-store on page 1837](#)
- [diagnose user on page 1829](#)
- [diagnose vendor-mac on page 1851](#)
- [diagnose vmware on page 1852](#)
- [diagnose vpn ssl on page 1853](#)
- [diagnose wacs on page 1853](#)
- [diagnose wad on page 1854](#)
- [diagnose wadbd on page 1982](#)
- [diagnose waf on page 1983](#)
- [diagnose web-ui on page 1987](#)
- [diagnose webfilter on page 1984](#)

diagnose alertconsole

alertconsole

This topic includes the following commands:

- [diagnose alertconsole clear on page 1495](#)
- [diagnose alertconsole fgd-retrieve on page 1495](#)
- [diagnose alertconsole list on page 1495](#)

- [diagnose alertconsole test on page 1495](#)

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 1496](#)
- [diagnose antivirus outbreak-prevention on page 1496](#)
- [diagnose antivirus outbreak-prevention statistics on page 1496](#)
- [diagnose antivirus outbreak-prevention statistics flush on page 1496](#)
- [diagnose antivirus outbreak-prevention statistics list on page 1496](#)
- [diagnose antivirus quarantine on page 1496](#)
- [diagnose antivirus quarantine delete on page 1497](#)

- [diagnose antivirus quarantine list on page 1497](#)
- [diagnose antivirus quarantine purge on page 1497](#)
- [diagnose antivirus test on page 1497](#)

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 1498](#)

diagnose automation test

Test automation stitches.

```
diagnose automation test
```

diagnose autoupdate

Automatic updates.

This topic includes the following commands:

- [diagnose autoupdate downgrade on page 1498](#)
- [diagnose autoupdate downgrade disable on page 1498](#)
- [diagnose autoupdate downgrade enable on page 1499](#)
- [diagnose autoupdate status on page 1499](#)
- [diagnose autoupdate versions on page 1499](#)

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 casb

CASB diagnose commands.

This topic includes the following commands:

- [diagnose casb build on page 1500](#)
- [diagnose casb show on page 1500](#)
- [diagnose casb show app-details on page 1500](#)
- [diagnose casb show app-domains on page 1500](#)
- [diagnose casb show applications on page 1500](#)
- [diagnose casb show apps on page 1500](#)
- [diagnose casb show domains on page 1501](#)
- [diagnose casb show isdb on page 1501](#)
- [diagnose casb show isdb-all on page 1501](#)
- [diagnose casb show isdb-name on page 1501](#)
- [diagnose casb show isdb-uuid on page 1501](#)
- [diagnose casb verify on page 1501](#)
- [diagnose casb verify casb-isdb on page 1502](#)

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-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 debug

debug

This topic includes the following commands:

- [diagnose debug admin on page 1509](#)
- [diagnose debug admin error-log on page 1509](#)
- [diagnose debug application on page 1509](#)
- [diagnose debug application acd on page 1510](#)
- [diagnose debug application acid on page 1510](#)
- [diagnose debug application alarmd on page 1510](#)
- [diagnose debug application alertmail on page 1510](#)
- [diagnose debug application alicloud-ha on page 1510](#)
- [diagnose debug application alicloud-sdn on page 1511](#)
- [diagnose debug application authd on page 1511](#)
- [diagnose debug application autod on page 1511](#)
- [diagnose debug application awsd on page 1511](#)
- [diagnose debug application azd on page 1512](#)
- [diagnose debug application azd-ha on page 1512](#)
- [diagnose debug application bfdd on page 1512](#)
- [diagnose debug application cert-update on page 1512](#)
- [diagnose debug application chassis on page 1513](#)
- [diagnose debug application clearpass on page 1513](#)
- [diagnose debug application cloudapid on page 1513](#)
- [diagnose debug application cloudinitd on page 1513](#)
- [diagnose debug application cmp on page 1513](#)
- [diagnose debug application crl-update on page 1514](#)
- [diagnose debug application crwl on page 1514](#)
- [diagnose debug application csfd on page 1514](#)
- [diagnose debug application ddnsd on page 1514](#)
- [diagnose debug application dhcp6c on page 1515](#)
- [diagnose debug application dhcp6r on page 1515](#)
- [diagnose debug application dhcp6s on page 1515](#)
- [diagnose debug application dhcpc on page 1515](#)
- [diagnose debug application dhcprelay on page 1516](#)

- [diagnose debug application dhcps on page 1516](#)
- [diagnose debug application dlpfingerprint on page 1516](#)
- [diagnose debug application dnp on page 1516](#)
- [diagnose debug application dnsproxy on page 1517](#)
- [diagnose debug application eap_proxy on page 1517](#)
- [diagnose debug application eap_supp on page 1517](#)
- [diagnose debug application est on page 1517](#)
- [diagnose debug application evpnd on page 1517](#)
- [diagnose debug application extenderd on page 1518](#)
- [diagnose debug application fclcd on page 1518](#)
- [diagnose debug application fcnacd on page 1518](#)
- [diagnose debug application fds_notify on page 1518](#)
- [diagnose debug application fgd_alert on page 1519](#)
- [diagnose debug application fgfmd on page 1519](#)
- [diagnose debug application fgtlogd on page 1519](#)
- [diagnose debug application fnbamd on page 1519](#)
- [diagnose debug application foauthd on page 1520](#)
- [diagnose debug application forticldd on page 1520](#)
- [diagnose debug application forticron on page 1520](#)
- [diagnose debug application fsd on page 1520](#)
- [diagnose debug application fsso_ldap on page 1520](#)
- [diagnose debug application fssod on page 1521](#)
- [diagnose debug application fsvrd on page 1521](#)
- [diagnose debug application ftm-push on page 1521](#)
- [diagnose debug application garpd on page 1521](#)
- [diagnose debug application gcpcd on page 1522](#)
- [diagnose debug application hamonitor on page 1522](#)
- [diagnose debug application harelay on page 1522](#)
- [diagnose debug application hasync on page 1522](#)
- [diagnose debug application hatalk on page 1523](#)
- [diagnose debug application httpsd on page 1523](#)
- [diagnose debug application ibmd on page 1523](#)
- [diagnose debug application icond on page 1523](#)
- [diagnose debug application imap on page 1524](#)
- [diagnose debug application init on page 1524](#)
- [diagnose debug application iotd on page 1524](#)
- [diagnose debug application ipamd on page 1524](#)
- [diagnose debug application ipamsd on page 1524](#)
- [diagnose debug application ipldbd on page 1525](#)
- [diagnose debug application ipsengine on page 1525](#)
- [diagnose debug application ipsmonitor on page 1525](#)
- [diagnose debug application ipsufd on page 1525](#)
- [diagnose debug application iptables on page 1526](#)

- [diagnose debug application kmiglogd on page 1526](#)
- [diagnose debug application kmipd on page 1526](#)
- [diagnose debug application kubed on page 1526](#)
- [diagnose debug application l2tp on page 1527](#)
- [diagnose debug application link-monitor on page 1527](#)
- [diagnose debug application link-monitor-passive on page 1527](#)
- [diagnose debug application lldptx on page 1527](#)
- [diagnose debug application locallogd on page 1527](#)
- [diagnose debug application lpmd on page 1528](#)
- [diagnose debug application miglogd on page 1528](#)
- [diagnose debug application mrd on page 1528](#)
- [diagnose debug application nethsm on page 1528](#)
- [diagnose debug application netxd on page 1529](#)
- [diagnose debug application nntp on page 1529](#)
- [diagnose debug application nodejs on page 1529](#)
- [diagnose debug application npd on page 1529](#)
- [diagnose debug application ntnxd on page 1530](#)
- [diagnose debug application ntpd on page 1530](#)
- [diagnose debug application oaas_agent on page 1530](#)
- [diagnose debug application ocid on page 1530](#)
- [diagnose debug application openstackd on page 1531](#)
- [diagnose debug application ovrd on page 1531](#)
- [diagnose debug application pcpd on page 1531](#)
- [diagnose debug application pop3 on page 1531](#)
- [diagnose debug application ppp on page 1531](#)
- [diagnose debug application pppoe on page 1532](#)
- [diagnose debug application pptp on page 1532](#)
- [diagnose debug application pptpc on page 1532](#)
- [diagnose debug application proxy on page 1532](#)
- [diagnose debug application ptpd on page 1533](#)
- [diagnose debug application quarantine on page 1533](#)
- [diagnose debug application radius-das on page 1533](#)
- [diagnose debug application radiusd on page 1533](#)
- [diagnose debug application radvd on page 1534](#)
- [diagnose debug application reportd on page 1534](#)
- [diagnose debug application route-tag on page 1534](#)
- [diagnose debug application rt-router on page 1534](#)
- [diagnose debug application samld on page 1534](#)
- [diagnose debug application sapd on page 1535](#)
- [diagnose debug application sccp on page 1535](#)
- [diagnose debug application scep on page 1535](#)
- [diagnose debug application sdncd on page 1535](#)
- [diagnose debug application sdwan on page 1536](#)

- [diagnose debug application sepmd on page 1536](#)
- [diagnose debug application server-probe on page 1536](#)
- [diagnose debug application sessionsync on page 1536](#)
- [diagnose debug application sflowd on page 1537](#)
- [diagnose debug application sfupgraded on page 1537](#)
- [diagnose debug application sip on page 1537](#)
- [diagnose debug application smbcd on page 1537](#)
- [diagnose debug application smtp on page 1537](#)
- [diagnose debug application snmpd on page 1538](#)
- [diagnose debug application spareblock on page 1538](#)
- [diagnose debug application speedtest on page 1538](#)
- [diagnose debug application speedtestd on page 1538](#)
- [diagnose debug application sshd on page 1539](#)
- [diagnose debug application syslogd on page 1539](#)
- [diagnose debug application tvc on page 1539](#)
- [diagnose debug application update on page 1539](#)
- [diagnose debug application uploadd on page 1540](#)
- [diagnose debug application urlfilter on page 1540](#)
- [diagnose debug application vmtoolsd on page 1540](#)
- [diagnose debug application vmwd on page 1540](#)
- [diagnose debug application vned on page 1540](#)
- [diagnose debug application vpd on page 1541](#)
- [diagnose debug application vrrpd on page 1541](#)
- [diagnose debug application wabcs on page 1541](#)
- [diagnose debug application waocs on page 1541](#)
- [diagnose debug application wccpd on page 1542](#)
- [diagnose debug application wf_monitor on page 1542](#)
- [diagnose debug authd on page 1542](#)
- [diagnose debug authd clear on page 1542](#)
- [diagnose debug authd fsso on page 1542](#)
- [diagnose debug authd fsso add-address on page 1543](#)
- [diagnose debug authd fsso clear-logons on page 1543](#)
- [diagnose debug authd fsso del-address on page 1543](#)
- [diagnose debug authd fsso filter on page 1543](#)
- [diagnose debug authd fsso filter clear on page 1543](#)
- [diagnose debug authd fsso filter group on page 1544](#)
- [diagnose debug authd fsso filter server on page 1544](#)
- [diagnose debug authd fsso filter source on page 1544](#)
- [diagnose debug authd fsso filter user on page 1544](#)
- [diagnose debug authd fsso flush-address on page 1544](#)
- [diagnose debug authd fsso flush-address-all on page 1545](#)
- [diagnose debug authd fsso list on page 1545](#)
- [diagnose debug authd fsso refresh-groups on page 1545](#)

- [diagnose debug authd fsso refresh-logons on page 1545](#)
- [diagnose debug authd fsso server-status on page 1545](#)
- [diagnose debug authd fsso show-address on page 1545](#)
- [diagnose debug authd fsso summary on page 1546](#)
- [diagnose debug authd memory on page 1546](#)
- [diagnose debug backtrace on page 1546](#)
- [diagnose debug cli on page 1546](#)
- [diagnose debug cloudinit on page 1546](#)
- [diagnose debug cloudinit clear on page 1546](#)
- [diagnose debug cloudinit show on page 1547](#)
- [diagnose debug cmdb-trace on page 1547](#)
- [diagnose debug cmdb-walk on page 1547](#)
- [diagnose debug config-error-log on page 1547](#)
- [diagnose debug config-error-log clear on page 1547](#)
- [diagnose debug config-error-log read on page 1548](#)
- [diagnose debug console on page 1548](#)
- [diagnose debug console no-user-log-msg on page 1548](#)
- [diagnose debug console no-user-log-msg disable on page 1548](#)
- [diagnose debug console no-user-log-msg enable on page 1548](#)
- [diagnose debug console retry-log-msg on page 1548](#)
- [diagnose debug console retry-log-msg disable on page 1549](#)
- [diagnose debug console retry-log-msg enable on page 1549](#)
- [diagnose debug console send on page 1549](#)
- [diagnose debug console timestamp on page 1549](#)
- [diagnose debug console timestamp disable on page 1549](#)
- [diagnose debug console timestamp enable on page 1550](#)
- [diagnose debug crashlog on page 1550](#)
- [diagnose debug crashlog clear on page 1550](#)
- [diagnose debug crashlog get on page 1550](#)
- [diagnose debug crashlog history on page 1550](#)
- [diagnose debug crashlog interval on page 1550](#)
- [diagnose debug disable on page 1551](#)
- [diagnose debug duration on page 1551](#)
- [diagnose debug enable on page 1551](#)
- [diagnose debug flow on page 1551](#)
- [diagnose debug flow filter on page 1551](#)
- [diagnose debug flow filter addr on page 1552](#)
- [diagnose debug flow filter clear on page 1552](#)
- [diagnose debug flow filter daddr on page 1552](#)
- [diagnose debug flow filter dport on page 1552](#)
- [diagnose debug flow filter negate on page 1553](#)
- [diagnose debug flow filter negate addr on page 1553](#)
- [diagnose debug flow filter negate daddr on page 1553](#)

- [diagnose debug flow filter negate dport on page 1554](#)
- [diagnose debug flow filter negate port on page 1554](#)
- [diagnose debug flow filter negate proto on page 1554](#)
- [diagnose debug flow filter negate saddr on page 1554](#)
- [diagnose debug flow filter negate sport on page 1555](#)
- [diagnose debug flow filter negate vd on page 1555](#)
- [diagnose debug flow filter port on page 1555](#)
- [diagnose debug flow filter proto on page 1555](#)
- [diagnose debug flow filter saddr on page 1556](#)
- [diagnose debug flow filter sport on page 1556](#)
- [diagnose debug flow filter vd on page 1556](#)
- [diagnose debug flow filter vd-name on page 1557](#)
- [diagnose debug flow filter6 on page 1557](#)
- [diagnose debug flow filter6 addr on page 1557](#)
- [diagnose debug flow filter6 clear on page 1558](#)
- [diagnose debug flow filter6 daddr on page 1558](#)
- [diagnose debug flow filter6 dport on page 1558](#)
- [diagnose debug flow filter6 negate on page 1559](#)
- [diagnose debug flow filter6 negate addr on page 1559](#)
- [diagnose debug flow filter6 negate daddr on page 1559](#)
- [diagnose debug flow filter6 negate dport on page 1559](#)
- [diagnose debug flow filter6 negate port on page 1560](#)
- [diagnose debug flow filter6 negate proto on page 1560](#)
- [diagnose debug flow filter6 negate saddr on page 1560](#)
- [diagnose debug flow filter6 negate sport on page 1560](#)
- [diagnose debug flow filter6 negate vd on page 1561](#)
- [diagnose debug flow filter6 port on page 1561](#)
- [diagnose debug flow filter6 proto on page 1561](#)
- [diagnose debug flow filter6 saddr on page 1561](#)
- [diagnose debug flow filter6 sport on page 1562](#)
- [diagnose debug flow filter6 vd on page 1562](#)
- [diagnose debug flow filter6 vd-name on page 1562](#)
- [diagnose debug flow show on page 1563](#)
- [diagnose debug flow show function-name on page 1563](#)
- [diagnose debug flow show function-name disable on page 1563](#)
- [diagnose debug flow show function-name enable on page 1563](#)
- [diagnose debug flow trace on page 1563](#)
- [diagnose debug flow trace start on page 1564](#)
- [diagnose debug flow trace start6 on page 1564](#)
- [diagnose debug flow trace stop on page 1564](#)
- [diagnose debug flow trace stop6 on page 1564](#)
- [diagnose debug fortism on page 1564](#)
- [diagnose debug fortism enable on page 1565](#)

- [diagnose debug fsso-polling on page 1565](#)
- [diagnose debug fsso-polling client on page 1565](#)
- [diagnose debug fsso-polling detail on page 1565](#)
- [diagnose debug fsso-polling group on page 1565](#)
- [diagnose debug fsso-polling refresh-user on page 1566](#)
- [diagnose debug fsso-polling set-log-source on page 1566](#)
- [diagnose debug fsso-polling summary on page 1566](#)
- [diagnose debug fsso-polling user on page 1566](#)
- [diagnose debug info on page 1566](#)
- [diagnose debug kernel on page 1567](#)
- [diagnose debug kernel ha on page 1567](#)
- [diagnose debug kernel level on page 1567](#)
- [diagnose debug kernel log on page 1567](#)
- [diagnose debug kernel log clear on page 1567](#)
- [diagnose debug kernel log show on page 1568](#)
- [diagnose debug kernel sysrq on page 1568](#)
- [diagnose debug kernel sysrq command on page 1568](#)
- [diagnose debug kernel sysrq command crash on page 1568](#)
- [diagnose debug kernel sysrq disable on page 1568](#)
- [diagnose debug kernel sysrq enable on page 1568](#)
- [diagnose debug kernel sysrq status on page 1569](#)
- [diagnose debug rating on page 1569](#)
- [diagnose debug remote-extender on page 1569](#)
- [diagnose debug remote-extender extenderd on page 1569](#)
- [diagnose debug remote-extender modem-manager on page 1569](#)
- [diagnose debug report on page 1570](#)
- [diagnose debug report reset on page 1570](#)
- [diagnose debug reset on page 1570](#)
- [diagnose debug sdnc on page 1570](#)
- [diagnose debug sdnc valgrind on page 1570](#)
- [diagnose debug sdnc valgrind disable on page 1570](#)
- [diagnose debug sdnc valgrind enable on page 1571](#)
- [diagnose debug sdnc valgrind log on page 1571](#)
- [diagnose debug sdnc valgrind log clear on page 1571](#)
- [diagnose debug sdnc valgrind log show on page 1571](#)
- [diagnose debug sdnc valgrind memcheck on page 1571](#)
- [diagnose debug sdnc valgrind memcheck_less on page 1571](#)
- [diagnose debug sdnc valgrind status on page 1572](#)
- [diagnose debug sql-log-error on page 1572](#)
- [diagnose debug sql-log-error clear on page 1572](#)
- [diagnose debug sql-log-error read on page 1572](#)
- [diagnose debug sql-log-error status on page 1572](#)
- [diagnose debug traffic on page 1572](#)

- [diagnose debug traffic dump-debug on page 1573](#)
- [diagnose debug traffic history on page 1573](#)
- [diagnose debug traffic interface on page 1573](#)
- [diagnose debug traffic peek on page 1573](#)
- [diagnose debug urlfilter on page 1573](#)
- [diagnose debug urlfilter src-addr on page 1574](#)
- [diagnose debug urlfilter test-url on page 1574](#)
- [diagnose debug urlfilter valgrind on page 1574](#)
- [diagnose debug urlfilter valgrind disable on page 1574](#)
- [diagnose debug urlfilter valgrind enable on page 1574](#)
- [diagnose debug urlfilter valgrind log on page 1575](#)
- [diagnose debug urlfilter valgrind log clear on page 1575](#)
- [diagnose debug urlfilter valgrind log show on page 1575](#)
- [diagnose debug urlfilter valgrind memcheck on page 1575](#)
- [diagnose debug urlfilter valgrind memcheck_less on page 1575](#)
- [diagnose debug urlfilter valgrind status on page 1575](#)
- [diagnose debug user on page 1576](#)
- [diagnose debug user hash on page 1576](#)
- [diagnose debug user list on page 1576](#)
- [diagnose debug vm-print-license on page 1576](#)

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 crwl

HTTP/S preload feature crawler.

```
diagnose debug application crwl <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>>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	
<serial <serialnum> ip <ip> direction <up down>>	Filter by serial number, IP, or stream direction.	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>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	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 fcld

Fclicense daemon.

```
diagnose debug application fcld <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 fnbamd

Fortiproxy 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 forticld

FortiCloud daemon.

```
diagnose debug application forticld <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 fsd

Forti-start daemon.

```
diagnose debug application fsd <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 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 ipdbd

Ipdbd daemon.

```
diagnose debug application ipdbd <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 iptables

iptables debug trace

```
diagnose debug application iptables <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 lldptx

Link Layer Discovery Protocol (LLDP) Transmitter

```
diagnose debug application lldptx <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 nethsm

NETHSM daemon.

```
diagnose debug application nethsm <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 rt-router

RT Router daemon.

```
diagnose debug application rt-router <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 sdncd

SDN Connector daemon.

```
diagnose debug application sdncd <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 syslogd

syslogd daemon.

```
diagnose debug application syslogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Debug level.	string	

diagnose debug application tvc

SSL-VPN client

```
diagnose debug application tvc <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 vmtoolsd

vmtoolsd daemon.

```
diagnose debug application vmtoolsd <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 vpd

VPN policy daemon.

```
diagnose debug application vpd <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 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+..*adgrp> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<adgrp1+adgrp2+..*adgrp>	AD groups.	string	
<xxx.xxx.xxx.xxx>	IP start 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+..*adgrp> <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<adgrp1+adgrp2+..*adgrp>	AD groups.	string	
<xxx.xxx.xxx.xxx>	IP start 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>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (range from).	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 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>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Host IP (ip1/from).	string	

diagnose debug flow filter clear

Clear filter.

```
diagnose debug flow filter clear
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter daddr

Destination IP address.

```
diagnose debug flow filter daddr <xxx.xxx.xxx.xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	

diagnose debug flow filter dport

Destination port.

```
diagnose debug flow filter dport <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx>	Destination port (from).	string	

diagnose debug flow filter negate

Inverse filter.

```
diagnose debug flow filter negate
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate addr

Inverse host IP.

```
diagnose debug flow filter negate addr
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate daddr

Inverse dest IP.

```
diagnose debug flow filter negate daddr
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate dport

Inverse dest port.

```
diagnose debug flow filter negate dport
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate port

Inverse port.

```
diagnose debug flow filter negate port
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate proto

Inverse protocol.

```
diagnose debug flow filter negate proto
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate saddr

Inverse source IP.

```
diagnose debug flow filter negate saddr
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate sport

Inverse source port.

```
diagnose debug flow filter negate sport
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter negate vd

Inverse virtual domain.

```
diagnose debug flow filter negate vd
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter port

port

```
diagnose debug flow filter port <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx>	Port (from).	string	

diagnose debug flow filter proto

Protocol number.

```
diagnose debug flow filter proto <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

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>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	

diagnose debug flow filter sport

Source port.

```
diagnose debug flow filter sport <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx>	Source port (from).	string	

diagnose debug flow filter vd

Index of virtual domain.

```
diagnose debug flow filter vd <xxx>
```




The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

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 <...>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<...>	Name of virtual domain.	string	

diagnose debug flow filter6

Trace packet with IPv6 filter.

```
diagnose debug flow filter6
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 addr

IPv6 address.

```
diagnose debug flow filter6 addr <xxx:xxx::xxx:xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Host IPv6 (from).	string	

diagnose debug flow filter6 clear

Clear IPv6 filter.

```
diagnose debug flow filter6 clear
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 daddr

Destination IP address.

```
diagnose debug flow filter6 daddr <xxx:xxx::xxx:xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Destination IP (from).	string	

diagnose debug flow filter6 dport

Destination port.

```
diagnose debug flow filter6 dport <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx>	Destination port (from).	string	

diagnose debug flow filter6 negate

Inverse IPv6 filter.

```
diagnose debug flow filter6 negate
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate addr

Inverse host IP.

```
diagnose debug flow filter6 negate addr
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate daddr

Inverse dest IP.

```
diagnose debug flow filter6 negate daddr
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate dport

Inverse dest port.

```
diagnose debug flow filter6 negate dport
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate port

Inverse port.

```
diagnose debug flow filter6 negate port
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate proto

Inverse protocol.

```
diagnose debug flow filter6 negate proto
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate saddr

Inverse source IP.

```
diagnose debug flow filter6 negate saddr
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate sport

Inverse source port.

```
diagnose debug flow filter6 negate sport
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 negate vd

Inverse virtual domain.

```
diagnose debug flow filter6 negate vd
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

diagnose debug flow filter6 port

port

```
diagnose debug flow filter6 port <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx>	Port (from).	string	

diagnose debug flow filter6 proto

Protocol number.

```
diagnose debug flow filter6 proto <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

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>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Source IP (from).	string	

diagnose debug flow filter6 sport

Source port.

```
diagnose debug flow filter6 sport <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

Parameter	Description	Type	Size
<xxx>	Source port (from).	string	

diagnose debug flow filter6 vd

Index of virtual domain.

```
diagnose debug flow filter6 vd <xxx>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

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 <...>
```



The command may cause high CPU and memory usage. To close, run `diagnose debug flow filter clear`.

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 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 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 log

Interact with kernel log

```
diagnose debug kernel log
```

diagnose debug kernel log clear

Clear the kernel log

```
diagnose debug kernel log clear
```

diagnose debug kernel log show

Dump the kernel log

```
diagnose debug kernel log show
```

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 remote-extender

remote-extender

```
diagnose debug remote-extender
```

diagnose debug remote-extender extenderd

Debug extenderd level.

```
diagnose debug remote-extender extenderd <Integer>
```

Parameter	Description	Type	Size
<Integer>	extenderd debug level.	string	

diagnose debug remote-extender modem-manager

Debug modem-manager level.

```
diagnose debug remote-extender modem-manager <Integer>
```

Parameter	Description	Type	Size
<Integer>	modem-manager debug level.	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 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 disktest

Disk test

This topic includes the following commands:

- [diagnose disktest block on page 1577](#)
- [diagnose disktest block 1 on page 1577](#)
- [diagnose disktest block 16 on page 1577](#)
- [diagnose disktest block 256 on page 1577](#)
- [diagnose disktest block 4 on page 1577](#)
- [diagnose disktest block 64 on page 1577](#)

- [diagnose disktest device on page 1578](#)
- [diagnose disktest run on page 1578](#)
- [diagnose disktest size on page 1578](#)
- [diagnose disktest time on page 1578](#)

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 emailfilter

emailfilter

This topic includes the following commands:

- [diagnose emailfilter bword on page 1579](#)
- [diagnose emailfilter bword matchfilter on page 1579](#)
- [diagnose emailfilter fortishield on page 1579](#)
- [diagnose emailfilter fortishield servers on page 1579](#)
- [diagnose emailfilter fortishield statistics on page 1580](#)
- [diagnose emailfilter fortishield statistics flush on page 1580](#)
- [diagnose emailfilter fortishield statistics list on page 1580](#)

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 1582](#)
- [diagnose endpoint avatar allow-nodisk on page 1583](#)
- [diagnose endpoint avatar cleanup on page 1583](#)
- [diagnose endpoint avatar find on page 1583](#)
- [diagnose endpoint avatar find fingerprint on page 1583](#)
- [diagnose endpoint avatar find uid on page 1583](#)
- [diagnose endpoint avatar list on page 1584](#)
- [diagnose endpoint avatar list active on page 1584](#)
- [diagnose endpoint avatar list all on page 1584](#)

- [diagnose endpoint avatar list inactive on page 1584](#)
- [diagnose endpoint avatar purge-all on page 1585](#)
- [diagnose endpoint debug-zone on page 1585](#)
- [diagnose endpoint debug-zone background-debug on page 1585](#)
- [diagnose endpoint debug-zone dump on page 1585](#)
- [diagnose endpoint debug-zone set-lls-quota on page 1585](#)
- [diagnose endpoint ec-shm on page 1586](#)
- [diagnose endpoint ec-shm delete on page 1586](#)
- [diagnose endpoint ec-shm find-by-ipvd on page 1586](#)
- [diagnose endpoint ec-shm find-by-uid on page 1586](#)
- [diagnose endpoint ec-shm list on page 1587](#)
- [diagnose endpoint ec-shm summary on page 1587](#)
- [diagnose endpoint ec-shm update-by-json on page 1587](#)
- [diagnose endpoint fctems on page 1587](#)
- [diagnose endpoint fctems api-status on page 1588](#)
- [diagnose endpoint fctems api-status clear on page 1588](#)
- [diagnose endpoint fctems cloud-server on page 1588](#)
- [diagnose endpoint fctems custom on page 1588](#)
- [diagnose endpoint fctems ec-shm-dump on page 1589](#)
- [diagnose endpoint fctems get-pub-addr on page 1589](#)
- [diagnose endpoint fctems info on page 1589](#)
- [diagnose endpoint fctems info pause on page 1589](#)
- [diagnose endpoint fctems info pre-master-key on page 1589](#)
- [diagnose endpoint fctems info protocol on page 1590](#)
- [diagnose endpoint fctems info repeat on page 1590](#)
- [diagnose endpoint fctems info repeat data-in on page 1590](#)
- [diagnose endpoint fctems info repeat data-out on page 1590](#)
- [diagnose endpoint fctems info repeat header-in on page 1590](#)
- [diagnose endpoint fctems info repeat header-out on page 1591](#)
- [diagnose endpoint fctems info repeat ssl-data-in on page 1591](#)
- [diagnose endpoint fctems info repeat ssl-data-out on page 1591](#)
- [diagnose endpoint fctems info repeat textinfo on page 1591](#)
- [diagnose endpoint fctems info reset on page 1592](#)
- [diagnose endpoint fctems info resume on page 1592](#)
- [diagnose endpoint fctems json on page 1592](#)
- [diagnose endpoint fctems json deep-inspect-cert-sync on page 1592](#)
- [diagnose endpoint fctems json gateway-mac-request on page 1592](#)
- [diagnose endpoint fctems queue-complete-calls on page 1592](#)
- [diagnose endpoint fctems test-authorization on page 1593](#)
- [diagnose endpoint fctems test-connectivity on page 1593](#)
- [diagnose endpoint fctems wss-cert-skip-check on page 1593](#)
- [diagnose endpoint filter on page 1593](#)
- [diagnose endpoint filter avatar-fingerprint on page 1593](#)

- [diagnose endpoint filter clear on page 1594](#)
- [diagnose endpoint filter ems-sn on page 1594](#)
- [diagnose endpoint filter ftcl-uid on page 1594](#)
- [diagnose endpoint filter list on page 1594](#)
- [diagnose endpoint filter record-debug-log on page 1594](#)
- [diagnose endpoint filter show-large-data on page 1595](#)
- [diagnose endpoint lls-comm on page 1595](#)
- [diagnose endpoint lls-comm connect on page 1595](#)
- [diagnose endpoint lls-comm disconnect on page 1595](#)
- [diagnose endpoint lls-comm recv on page 1595](#)
- [diagnose endpoint lls-comm send on page 1596](#)
- [diagnose endpoint lls-comm send echo on page 1596](#)
- [diagnose endpoint lls-comm send general on page 1596](#)
- [diagnose endpoint lls-comm send general get-index on page 1596](#)
- [diagnose endpoint lls-comm send general register on page 1596](#)
- [diagnose endpoint lls-comm send general unregister on page 1596](#)
- [diagnose endpoint lls-comm send ping on page 1597](#)
- [diagnose endpoint lls-comm send ping set-interval on page 1597](#)
- [diagnose endpoint lls-comm send ztna on page 1597](#)
- [diagnose endpoint lls-comm send ztna find-ip-vdom on page 1597](#)
- [diagnose endpoint lls-comm send ztna find-uid on page 1597](#)
- [diagnose endpoint lls-comm send ztna message-format on page 1598](#)
- [diagnose endpoint lls-comm send ztna subscribe-all on page 1598](#)
- [diagnose endpoint lls-comm send ztna unsubscribe-all on page 1598](#)
- [diagnose endpoint lls-comm send ztna unsubscribe-uid on page 1598](#)
- [diagnose endpoint lls-comm status on page 1599](#)
- [diagnose endpoint tags on page 1599](#)
- [diagnose endpoint tags remove-by-id on page 1599](#)
- [diagnose endpoint tags remove-by-name on page 1599](#)
- [diagnose endpoint tags remove-by-name-legacy on page 1600](#)
- [diagnose endpoint tags remove-by-sn on page 1600](#)
- [diagnose endpoint tags test-common-tag-update on page 1600](#)

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	

Parameter	Description	Type	Size
<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 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 fdsm

FortiCloud/FortiManager Service.

This topic includes the following commands:

- [diagnose fdsm account-info on page 1601](#)
- [diagnose fdsm central-mgmt-status on page 1601](#)
- [diagnose fdsm cfg-diff on page 1601](#)

- [diagnose fdsm cfg-download on page 1602](#)
- [diagnose fdsm cfg-list on page 1602](#)
- [diagnose fdsm cfg-upload on page 1602](#)
- [diagnose fdsm contract-controller-update on page 1602](#)
- [diagnose fdsm fap-fsw-contract-download on page 1603](#)
- [diagnose fdsm fc-installer-download on page 1603](#)
- [diagnose fdsm fds-update on page 1603](#)
- [diagnose fdsm fmg-auto-discovery-status on page 1603](#)
- [diagnose fdsm forticlient-net-info on page 1603](#)
- [diagnose fdsm forticlient-update on page 1604](#)
- [diagnose fdsm fortiex-download on page 1604](#)
- [diagnose fdsm fortiex-latest-ver on page 1604](#)
- [diagnose fdsm fortisw-download on page 1604](#)
- [diagnose fdsm fortisw-latest-ver on page 1604](#)
- [diagnose fdsm ftk-activate on page 1605](#)
- [diagnose fdsm image-download on page 1605](#)
- [diagnose fdsm image-list on page 1605](#)
- [diagnose fdsm image-upgrade-matrix on page 1605](#)
- [diagnose fdsm log-controller-update on page 1605](#)
- [diagnose fdsm message-update on page 1606](#)
- [diagnose fdsm modem-list on page 1606](#)
- [diagnose fdsm report-download on page 1606](#)
- [diagnose fdsm report-list on page 1606](#)

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-contract-download

FAP/FSW contract information.

```
diagnose fdsm fap-fsw-contract-download <serial1*serial2*...>
```

Parameter	Description	Type	Size
<serial1*serial2*...>	Serial numbers of FAP/FSW devices	string	

diagnose fdsm fc-installer-download

Download FortiClient installer.

```
diagnose fdsm fc-installer-download <id>
```

Parameter	Description	Type	Size
<id>	Package 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 forticlient-net-info

FortiClient net information.

```
diagnose fdsm forticlient-net-info
```

diagnose fdsm forticlient-update

FortiClient update.

```
diagnose fdsm forticlient-update
```

diagnose fdsm fortix-download

Download FortiExtender image.

```
diagnose fdsm fortix-download <id>
```

Parameter	Description	Type	Size
<id>	Image ID	string	

diagnose fdsm fortix-latest-ver

Get most recent FortiExtender build information.

```
diagnose fdsm fortix-latest-ver <model>
```

Parameter	Description	Type	Size
<model>	Model name	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>
```


Parameter	Description	Type	Size
<model>	Model name	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 firewall

Firewall

This topic includes the following commands:

- [diagnose firewall auth on page 1608](#)
- [diagnose firewall auth clear on page 1609](#)
- [diagnose firewall auth filter on page 1609](#)

- [diagnose firewall auth filter clear on page 1609](#)
- [diagnose firewall auth filter group on page 1609](#)
- [diagnose firewall auth filter mac on page 1609](#)
- [diagnose firewall auth filter method on page 1610](#)
- [diagnose firewall auth filter policy on page 1610](#)
- [diagnose firewall auth filter source on page 1610](#)
- [diagnose firewall auth filter source6 on page 1610](#)
- [diagnose firewall auth filter user on page 1611](#)
- [diagnose firewall auth ipv6 on page 1611](#)
- [diagnose firewall auth ipv6 clear on page 1611](#)
- [diagnose firewall auth ipv6 list on page 1611](#)
- [diagnose firewall auth list on page 1611](#)
- [diagnose firewall auth mac on page 1611](#)
- [diagnose firewall auth mac clear on page 1612](#)
- [diagnose firewall auth mac list on page 1612](#)
- [diagnose firewall dynamic on page 1612](#)
- [diagnose firewall dynamic address on page 1612](#)
- [diagnose firewall dynamic list on page 1612](#)
- [diagnose firewall dynamic test-common-tag-update on page 1613](#)
- [diagnose firewall dynamic6 on page 1613](#)
- [diagnose firewall dynamic6 address on page 1613](#)
- [diagnose firewall dynamic6 list on page 1613](#)
- [diagnose firewall fqdn on page 1613](#)
- [diagnose firewall fqdn get-ip on page 1614](#)
- [diagnose firewall fqdn get-mac on page 1614](#)
- [diagnose firewall fqdn getinfo-ip on page 1614](#)
- [diagnose firewall fqdn getinfo-mac on page 1614](#)
- [diagnose firewall fqdn list-all on page 1614](#)
- [diagnose firewall fqdn list-ip on page 1615](#)
- [diagnose firewall fqdn list-mac on page 1615](#)
- [diagnose firewall fqdn6 on page 1615](#)
- [diagnose firewall fqdn6 get on page 1615](#)
- [diagnose firewall fqdn6 list on page 1615](#)
- [diagnose firewall internet-service on page 1615](#)
- [diagnose firewall internet-service list on page 1616](#)
- [diagnose firewall internet-service-app-ctrl on page 1616](#)
- [diagnose firewall internet-service-cache on page 1616](#)
- [diagnose firewall internet-service-cache list on page 1616](#)
- [diagnose firewall internet-service-custom on page 1616](#)
- [diagnose firewall internet-service-custom list on page 1617](#)
- [diagnose firewall internet-service-disable on page 1617](#)
- [diagnose firewall internet-service-disable list on page 1617](#)
- [diagnose firewall internet-service-extension on page 1617](#)

- [diagnose firewall internet-service-extension list on page 1617](#)
- [diagnose firewall internet-service-prio-id on page 1618](#)
- [diagnose firewall internet-service-prio-id list on page 1618](#)
- [diagnose firewall internet-service6 on page 1618](#)
- [diagnose firewall internet-service6 list on page 1618](#)
- [diagnose firewall internet-service6-cache on page 1618](#)
- [diagnose firewall internet-service6-cache list on page 1618](#)
- [diagnose firewall internet-service6-custom on page 1619](#)
- [diagnose firewall internet-service6-custom list on page 1619](#)
- [diagnose firewall internet-service6-disable on page 1619](#)
- [diagnose firewall internet-service6-disable list on page 1619](#)
- [diagnose firewall internet-service6-extension on page 1619](#)
- [diagnose firewall internet-service6-extension list on page 1620](#)
- [diagnose firewall internet-service6-prio-id on page 1620](#)
- [diagnose firewall internet-service6-prio-id list on page 1620](#)
- [diagnose firewall ipgeo on page 1620](#)
- [diagnose firewall ipgeo copyright-notice on page 1620](#)
- [diagnose firewall ipgeo country-list on page 1620](#)
- [diagnose firewall ipgeo ip-list on page 1621](#)
- [diagnose firewall ipgeo ip2country on page 1621](#)
- [diagnose firewall ipgeo override on page 1621](#)
- [diagnose firewall network-service-dynamic on page 1621](#)
- [diagnose firewall network-service-dynamic list on page 1621](#)
- [diagnose firewall nslookup on page 1622](#)
- [diagnose firewall shaper on page 1622](#)
- [diagnose firewall shaper per-ip-shaper on page 1622](#)
- [diagnose firewall shaper per-ip-shaper clear on page 1622](#)
- [diagnose firewall shaper per-ip-shaper list on page 1622](#)
- [diagnose firewall shaper per-ip-shaper state on page 1622](#)
- [diagnose firewall shaper per-ip-shaper stats on page 1623](#)
- [diagnose firewall shaper traffic-shaper on page 1623](#)
- [diagnose firewall shaper traffic-shaper list on page 1623](#)
- [diagnose firewall shaper traffic-shaper stats on page 1623](#)
- [diagnose firewall shaper traffic-shaper stats clear on page 1623](#)
- [diagnose firewall shaper traffic-shaper stats list on page 1623](#)
- [diagnose firewall snat-ippool on page 1624](#)
- [diagnose firewall snat-ippool list on page 1624](#)
- [diagnose firewall snat-ippool list6 on page 1624](#)

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>
```

Parameter	Description	Type	Size
<method>	Valid method name: fsso, rso, ntlm, fw, wso, 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>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	IPv4 source (range from).	string	

diagnose firewall auth filter source6

IPv6 source address.

```
diagnose firewall auth filter source6 <xxxx::xxxx>
```

Parameter	Description	Type	Size
<xxxx::xxxx>	IPv6 source (range from).	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 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 get

Get and display one IPv6 FQDN address.

```
diagnose firewall fqdn6 get <name>
```

Parameter	Description	Type	Size
<name>	Address Name	string	

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-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 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 override

Print out all user defined IP geolocation data.

```
diagnose firewall ipgeo override
```

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 nslookup

Name server lookup.

```
diagnose firewall nslookup <FQDN> <DNS-server>
```

Parameter	Description	Type	Size
<FQDN>	FQDN.	string	
<DNS-server>	DNS-server.	string	

diagnose firewall shaper

shapers

```
diagnose firewall shaper
```

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 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 snat-ippool

All IP pool.

```
diagnose firewall snat-ippool
```

diagnose firewall snat-ippool list

List IPv4.

```
diagnose firewall snat-ippool list
```

diagnose firewall snat-ippool list6

List IPv6.

```
diagnose firewall snat-ippool list6
```

diagnose fortiguard-resources

FortiGuard resources.

This topic includes the following commands:

- [diagnose fortiguard-resources delete on page 1626](#)
- [diagnose fortiguard-resources delete app-categories on page 1626](#)
- [diagnose fortiguard-resources delete app-info on page 1626](#)
- [diagnose fortiguard-resources delete dlp-object on page 1626](#)
- [diagnose fortiguard-resources delete fortiap-end-of-support on page 1627](#)
- [diagnose fortiguard-resources delete fortitextender-end-of-support on page 1627](#)
- [diagnose fortiguard-resources delete fortigate-end-of-support on page 1627](#)
- [diagnose fortiguard-resources delete fortiswitch-end-of-support on page 1627](#)
- [diagnose fortiguard-resources delete ips-information on page 1627](#)
- [diagnose fortiguard-resources delete prefix-links on page 1628](#)
- [diagnose fortiguard-resources delete sprite-casb on page 1628](#)
- [diagnose fortiguard-resources delete sprite-isdb on page 1628](#)
- [diagnose fortiguard-resources delete sprite-map on page 1628](#)
- [diagnose fortiguard-resources delete static-links on page 1628](#)

- [diagnose fortiguard-resources delete wf-categories on page 1628](#)
- [diagnose fortiguard-resources delete-all on page 1629](#)
- [diagnose fortiguard-resources downloads on page 1629](#)
- [diagnose fortiguard-resources downloads disable on page 1629](#)
- [diagnose fortiguard-resources downloads enable on page 1629](#)
- [diagnose fortiguard-resources info on page 1629](#)
- [diagnose fortiguard-resources info app-categories on page 1629](#)
- [diagnose fortiguard-resources info app-info on page 1630](#)
- [diagnose fortiguard-resources info dlp-object on page 1630](#)
- [diagnose fortiguard-resources info fortiap-end-of-support on page 1630](#)
- [diagnose fortiguard-resources info fortixtender-end-of-support on page 1630](#)
- [diagnose fortiguard-resources info fortigate-end-of-support on page 1630](#)
- [diagnose fortiguard-resources info fortiswitch-end-of-support on page 1631](#)
- [diagnose fortiguard-resources info ips-information on page 1631](#)
- [diagnose fortiguard-resources info prefix-links on page 1631](#)
- [diagnose fortiguard-resources info sprite-casb.css on page 1631](#)
- [diagnose fortiguard-resources info sprite-casb.png on page 1631](#)
- [diagnose fortiguard-resources info sprite-isdb.css on page 1631](#)
- [diagnose fortiguard-resources info sprite-isdb.png on page 1632](#)
- [diagnose fortiguard-resources info sprite-map.css on page 1632](#)
- [diagnose fortiguard-resources info sprite-map.png on page 1632](#)
- [diagnose fortiguard-resources info static-links on page 1632](#)
- [diagnose fortiguard-resources info wf-categories on page 1632](#)
- [diagnose fortiguard-resources log on page 1632](#)
- [diagnose fortiguard-resources log all on page 1633](#)
- [diagnose fortiguard-resources log app-categories on page 1633](#)
- [diagnose fortiguard-resources log app-info on page 1633](#)
- [diagnose fortiguard-resources log fortiap-end-of-support on page 1633](#)
- [diagnose fortiguard-resources log fortixtender-end-of-support on page 1633](#)
- [diagnose fortiguard-resources log fortigate-end-of-support on page 1633](#)
- [diagnose fortiguard-resources log fortiswitch-end-of-support on page 1634](#)
- [diagnose fortiguard-resources log ips-information on page 1634](#)
- [diagnose fortiguard-resources log maintainer on page 1634](#)
- [diagnose fortiguard-resources log prefix-links on page 1634](#)
- [diagnose fortiguard-resources log sprite-casb on page 1634](#)
- [diagnose fortiguard-resources log sprite-isdb on page 1634](#)
- [diagnose fortiguard-resources log sprite-map on page 1635](#)
- [diagnose fortiguard-resources log static-links on page 1635](#)
- [diagnose fortiguard-resources log wf-categories on page 1635](#)
- [diagnose fortiguard-resources update on page 1635](#)
- [diagnose fortiguard-resources update app-categories on page 1635](#)
- [diagnose fortiguard-resources update app-info on page 1635](#)
- [diagnose fortiguard-resources update dlp-object on page 1636](#)

- [diagnose fortiguard-resources update fortiap-end-of-support on page 1636](#)
- [diagnose fortiguard-resources update fortixtender-end-of-support on page 1636](#)
- [diagnose fortiguard-resources update fortigate-end-of-support on page 1636](#)
- [diagnose fortiguard-resources update fortiswitch-end-of-support on page 1636](#)
- [diagnose fortiguard-resources update ips-information on page 1637](#)
- [diagnose fortiguard-resources update prefix-links on page 1637](#)
- [diagnose fortiguard-resources update sprite-casb on page 1637](#)
- [diagnose fortiguard-resources update sprite-isdb on page 1637](#)
- [diagnose fortiguard-resources update sprite-map on page 1637](#)
- [diagnose fortiguard-resources update static-links on page 1637](#)
- [diagnose fortiguard-resources update wf-categories on page 1638](#)

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 fortitender-end-of-support

FortiExtender product life cycle information.

```
diagnose fortiguard-resources log fortitender-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 fortitoken

FortiToken

This topic includes the following commands:

- [diagnose fortitoken debug on page 1638](#)
- [diagnose fortitoken debug disable on page 1638](#)
- [diagnose fortitoken debug enable on page 1638](#)
- [diagnose fortitoken info on page 1638](#)
- [diagnose fortitoken test on page 1639](#)

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	
<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 1640](#)
- [diagnose fortitoken-cloud debug on page 1640](#)
- [diagnose fortitoken-cloud debug disable on page 1640](#)
- [diagnose fortitoken-cloud debug enable on page 1640](#)
- [diagnose fortitoken-cloud debug info on page 1640](#)
- [diagnose fortitoken-cloud delete on page 1640](#)
- [diagnose fortitoken-cloud migrate-ftm on page 1641](#)
- [diagnose fortitoken-cloud server on page 1641](#)
- [diagnose fortitoken-cloud set-http on page 1641](#)
- [diagnose fortitoken-cloud show on page 1641](#)
- [diagnose fortitoken-cloud sync on page 1642](#)
- [diagnose fortitoken-cloud update on page 1642](#)

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>
```

Parameter	Description	Type	Size
<string>	User name.	string	

diagnose fortitoken-cloud migrate-ftm

Perform FTM license migration.

```
diagnose fortitoken-cloud migrate-ftm <string>
```

Parameter	Description	Type	Size
<string>	Enter command: show, start, abort, add-users, delete-users, 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>
```

Parameter	Description	Type	Size
<string>	Enter <server service users user>.	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 1642](#)
- [diagnose fortiview result on page 1643](#)
- [diagnose fortiview shaper-stats on page 1643](#)
- [diagnose fortiview sortby on page 1643](#)
- [diagnose fortiview time on page 1643](#)
- [diagnose fortiview view on page 1643](#)

diagnose fortiview device

device

```
diagnose fortiview device
```

diagnose fortiview result

result

```
diagnose fortiview result
```

diagnose fortiview shaper-stats

Fortiview shaper stats

```
diagnose fortiview shaper-stats
```

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 1644](#)
- [diagnose geoip geoip-query on page 1644](#)
- [diagnose geoip ip2country on page 1644](#)

- [diagnose geoip iprange on page 1644](#)
- [diagnose geoip iprange6 on page 1644](#)

diagnose geoip delete-geoip-db

Delete geography IP database currently saved on this FortiProxy 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 1645](#)
- [diagnose hardware deviceinfo on page 1645](#)
- [diagnose hardware deviceinfo disk on page 1646](#)
- [diagnose hardware deviceinfo nic on page 1646](#)
- [diagnose hardware deviceinfo nic-channel on page 1646](#)
- [diagnose hardware deviceinfo nic-stats on page 1646](#)
- [diagnose hardware deviceinfo tpm on page 1646](#)
- [diagnose hardware getcbp on page 1646](#)
- [diagnose hardware ioport on page 1647](#)
- [diagnose hardware lspci on page 1647](#)
- [diagnose hardware mii on page 1647](#)
- [diagnose hardware setcbp on page 1647](#)
- [diagnose hardware setpci on page 1647](#)
- [diagnose hardware sysinfo on page 1647](#)
- [diagnose hardware sysinfo conserve on page 1648](#)
- [diagnose hardware sysinfo cpu on page 1648](#)
- [diagnose hardware sysinfo interrupts on page 1648](#)
- [diagnose hardware sysinfo iomem on page 1648](#)
- [diagnose hardware sysinfo ioports on page 1648](#)
- [diagnose hardware sysinfo memory on page 1648](#)
- [diagnose hardware sysinfo mtrr on page 1649](#)
- [diagnose hardware sysinfo slab on page 1649](#)

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 deviceinfo tpm

Display information of TPM chip information.

```
diagnose hardware deviceinfo tpm
```

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 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 http-view

HTTP/S traffic daemon

This topic includes the following commands:

- [diagnose http-view clear on page 1649](#)
- [diagnose http-view debug on page 1649](#)
- [diagnose http-view log-show on page 1650](#)
- [diagnose http-view restart on page 1650](#)
- [diagnose http-view stats on page 1650](#)

diagnose http-view clear

Restart daemon, reset statistics & remove all history

```
diagnose http-view clear
```

diagnose http-view debug

Set debug level for daemon

```
diagnose http-view debug <debug level>
```

Parameter	Description	Type	Size
<debug level>	Hexadecimal number	string	

diagnose http-view log-show

Show log of daemon

```
diagnose http-view log-show <log generation> <time format>
```

Parameter	Description	Type	Size
<log generation>	Log generation: default 0	string	
<time format>	Time format: 0 for human readable and 1 for raw, default 0	string	

diagnose http-view restart

Restart the daemon and reset statistics

```
diagnose http-view restart
```

diagnose http-view stats

Show statistics.

```
diagnose http-view stats
```

diagnose ip

ip

This topic includes the following commands:

- [diagnose ip address on page 1651](#)
- [diagnose ip address add on page 1651](#)
- [diagnose ip address delete on page 1651](#)
- [diagnose ip address list on page 1652](#)
- [diagnose ip arp on page 1652](#)
- [diagnose ip arp add on page 1652](#)
- [diagnose ip arp delete on page 1652](#)
- [diagnose ip arp list on page 1652](#)
- [diagnose ip parp on page 1653](#)
- [diagnose ip parp list on page 1653](#)

- [diagnose ip route on page 1653](#)
- [diagnose ip route add on page 1653](#)
- [diagnose ip route delete on page 1653](#)
- [diagnose ip route list on page 1654](#)
- [diagnose ip route match on page 1654](#)
- [diagnose ip route verify on page 1654](#)
- [diagnose ip tcp on page 1654](#)
- [diagnose ip tcp list on page 1654](#)
- [diagnose ip udp on page 1655](#)
- [diagnose ip udp list on page 1655](#)

diagnose ip address

IP addresses.

```
diagnose ip address
```

diagnose ip address add

Add IP address.

```
diagnose ip address add <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 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.

```
diagnose ip arp
```

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 parp

Proxy-ARP table.

```
diagnose ip parp
```

diagnose ip parp list

Show Proxy-ARP table.

```
diagnose ip parp list
```

diagnose ip route

Routing table.

```
diagnose ip route
```

diagnose ip route add

Add static route.

```
diagnose ip route add <intf-name> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	

diagnose ip route delete

Delete static route.

```
diagnose ip route 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 route list

List routing table.

```
diagnose ip route list
```

diagnose ip route match

Match kernel route.

```
diagnose ip route match <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<XXX.XXX.XXX.XXX>	Destination address.	string	

diagnose ip route verify

Verify static route.

```
diagnose ip route verify <intf-name> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	

diagnose ip tcp

TCP sockets.

```
diagnose ip tcp
```

diagnose ip tcp list

List TCP sockets.

```
diagnose ip tcp list
```

diagnose ip udp

UDP sockets.

```
diagnose ip udp
```

diagnose ip udp list

List UDP sockets.

```
diagnose ip udp list
```

diagnose ip address

IP addresses.

This topic includes the following commands:

- [diagnose ip address add on page 1655](#)
- [diagnose ip address delete on page 1655](#)
- [diagnose ip address list on page 1656](#)

diagnose ip address add

Add IP address.

```
diagnose ip address add <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 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 1656](#)
- [diagnose ip arp delete on page 1656](#)
- [diagnose ip arp list on page 1657](#)

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 parp

Proxy-ARP table.

This topic includes the following commands:

- [diagnose ip parp list on page 1657](#)

diagnose ip parp list

Show Proxy-ARP table.

```
diagnose ip parp list
```

diagnose ip route

Routing table.

This topic includes the following commands:

- [diagnose ip route add on page 1658](#)
- [diagnose ip route delete on page 1658](#)
- [diagnose ip route list on page 1658](#)
- [diagnose ip route match on page 1658](#)
- [diagnose ip route verify on page 1658](#)

diagnose ip route add

Add static route.

```
diagnose ip route add <intf-name> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	

diagnose ip route delete

Delete static route.

```
diagnose ip route 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 route list

List routing table.

```
diagnose ip route list
```

diagnose ip route match

Match kernel route.

```
diagnose ip route match <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<XXX.XXX.XXX.XXX>	Destination address.	string	

diagnose ip route verify

Verify static route.

```
diagnose ip route verify <intf-name> <XXX.XXX.XXX.XXX>
```

Parameter	Description	Type	Size
<intf-name>	Interface Name.	string	
<XXX.XXX.XXX.XXX>	IP address.	string	

diagnose ip tcp

TCP sockets.

This topic includes the following commands:

- [diagnose ip tcp list on page 1659](#)

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 1659](#)

diagnose ip udp list

List UDP sockets.

```
diagnose ip udp list
```

diagnose ipsec

ipsec

This topic includes the following commands:

- [diagnose ipsec connect on page 1660](#)
- [diagnose ipsec list-conn on page 1660](#)
- [diagnose ipsec list-sa on page 1660](#)
- [diagnose ipsec p1-status on page 1660](#)
- [diagnose ipsec reload-ca on page 1660](#)
- [diagnose ipsec reload-ipsec on page 1661](#)

diagnose ipsec connect

connect sa

```
diagnose ipsec connect <phase1> <phase2>
```

Parameter	Description	Type	Size
<phase1>	phase1 name	string	
<phase2>	phase2 name	string	

diagnose ipsec list-conn

list ipsec conn

```
diagnose ipsec list-conn
```

diagnose ipsec list-sa

list ipsec sa

```
diagnose ipsec list-sa
```

diagnose ipsec p1-status

get phase1 tunnel status

```
diagnose ipsec p1-status
```

diagnose ipsec reload-ca

reload ipsec ca


```
diagnose ipsec reload-ca
```

diagnose ipsec reload-ipsec

reload ipsec

```
diagnose ipsec reload-ipsec
```

diagnose ipset

ipset

This topic includes the following commands:

- [diagnose ipset list on page 1661](#)

diagnose ipset list

list ipset entries

```
diagnose ipset list
```

diagnose iptables

iptables

This topic includes the following commands:

- [diagnose iptables dry-run on page 1661](#)
- [diagnose iptables list on page 1662](#)
- [diagnose iptables list6 on page 1662](#)
- [diagnose iptables refresh on page 1662](#)
- [diagnose iptables shaper on page 1662](#)
- [diagnose iptables shaper-stats on page 1662](#)

diagnose iptables dry-run

dump iptables rule

```
diagnose iptables dry-run
```

diagnose iptables list

list iptables

```
diagnose iptables list
```

diagnose iptables list6

list ip6tables

```
diagnose iptables list6
```

diagnose iptables refresh

refresh iptables

```
diagnose iptables refresh
```

diagnose iptables shaper

refresh shaper profile

```
diagnose iptables shaper
```

diagnose iptables shaper-stats

print shaper stats

```
diagnose iptables shaper-stats
```

diagnose ipv6

ipv6

This topic includes the following commands:

- [diagnose ipv6 address on page 1663](#)
- [diagnose ipv6 address add on page 1663](#)
- [diagnose ipv6 address delete on page 1663](#)
- [diagnose ipv6 address list on page 1664](#)
- [diagnose ipv6 devconf on page 1664](#)
- [diagnose ipv6 devconf accept-dad on page 1664](#)
- [diagnose ipv6 devconf disable_ipv6 on page 1664](#)
- [diagnose ipv6 neighbor-cache on page 1664](#)
- [diagnose ipv6 neighbor-cache add on page 1665](#)
- [diagnose ipv6 neighbor-cache delete on page 1665](#)
- [diagnose ipv6 neighbor-cache flush on page 1665](#)
- [diagnose ipv6 neighbor-cache list on page 1665](#)
- [diagnose ipv6 route on page 1666](#)
- [diagnose ipv6 route list on page 1666](#)

diagnose ipv6 address

IPv6 addresses.

```
diagnose ipv6 address
```

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 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 devconf

IPv6 device config.

```
diagnose ipv6 devconf
```

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 neighbor-cache

IPv6 neighbor-cache table.

```
diagnose ipv6 neighbor-cache
```

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 route

IPv6 routing table.

```
diagnose ipv6 route
```

diagnose ipv6 route list

List IPv6 routing table.

```
diagnose ipv6 route list
```

diagnose ipv6 address

IPv6 addresses.

This topic includes the following commands:

- [diagnose ipv6 address add on page 1666](#)
- [diagnose ipv6 address delete on page 1666](#)
- [diagnose ipv6 address list on page 1667](#)

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 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 neighbor-cache

IPv6 neighbor-cache table.

This topic includes the following commands:

- [diagnose ipv6 neighbor-cache add on page 1667](#)
- [diagnose ipv6 neighbor-cache delete on page 1667](#)
- [diagnose ipv6 neighbor-cache flush on page 1668](#)
- [diagnose ipv6 neighbor-cache list on page 1668](#)

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 route

IPv6 routing table.

This topic includes the following commands:

- [diagnose ipv6 route list on page 1668](#)

diagnose ipv6 route list

List IPv6 routing table.

```
diagnose ipv6 route list
```

diagnose lldprx

Link Layer Description Protocol (LLDP) Receiver diagnostics.

This topic includes the following commands:

- [diagnose lldprx config on page 1669](#)
- [diagnose lldprx neighbor on page 1669](#)
- [diagnose lldprx neighbor clear on page 1669](#)
- [diagnose lldprx neighbor details on page 1670](#)
- [diagnose lldprx neighbor summary on page 1670](#)
- [diagnose lldprx port on page 1670](#)
- [diagnose lldprx port details on page 1670](#)
- [diagnose lldprx port neighbor on page 1670](#)
- [diagnose lldprx port neighbor clear on page 1670](#)
- [diagnose lldprx port neighbor details on page 1671](#)
- [diagnose lldprx port neighbor summary on page 1671](#)
- [diagnose lldprx port summary on page 1671](#)
- [diagnose lldprx restart on page 1671](#)
- [diagnose lldprx stats on page 1671](#)
- [diagnose lldprx stats config on page 1671](#)
- [diagnose lldprx stats crash on page 1672](#)
- [diagnose lldprx stats manager on page 1672](#)
- [diagnose lldprx stats scan on page 1672](#)

diagnose lldprx config

Display LLDP configuration.

```
diagnose lldprx config
```

diagnose lldprx neighbor

Display LLDP neighbors.

```
diagnose lldprx neighbor
```

diagnose lldprx neighbor clear

Clear the LLDP from all ports.

```
diagnose lldprx neighbor clear
```

diagnose lldprx neighbor details

Display details of each LLDP neighbor.

```
diagnose lldprx neighbor details
```

diagnose lldprx neighbor summary

Display summary of each LLDP neighbor.

```
diagnose lldprx neighbor summary
```

diagnose lldprx port

Display summary information about each port with LLDP reception enabled.

```
diagnose lldprx port
```

diagnose lldprx port details

Display details of the LLDP enabled ports.

```
diagnose lldprx port details
```

diagnose lldprx port neighbor

Display information about each LLDP neighbor for one or more ports.

```
diagnose lldprx port neighbor
```

diagnose lldprx port neighbor clear

Clear the LLDP neighbor information for one or more ports.

```
diagnose lldprx port neighbor clear
```

diagnose lldprx port neighbor details

Display details of each LLDP neighbor for one or more ports.

```
diagnose lldprx port neighbor details
```

diagnose lldprx port neighbor summary

Display summary of each LLDP neighbor for one or more ports.

```
diagnose lldprx port neighbor summary
```

diagnose lldprx port summary

Display summary of the LLDP enabled ports.

```
diagnose lldprx port summary
```

diagnose lldprx restart

Restart the LLDPRX process

```
diagnose lldprx restart
```

diagnose lldprx stats

Display LLDPRX statistics.

```
diagnose lldprx stats
```

diagnose lldprx stats config

Display LLDPRX statistics for the configuration handling process.

```
diagnose lldprx stats config
```

diagnose lldprx stats crash

Display LLDPRX statistics for the crash log generating process.

```
diagnose lldprx stats crash
```

diagnose lldprx stats manager

Display LLDPRX statistics for the manager process.

```
diagnose lldprx stats manager
```

diagnose lldprx stats scan

Display LLDPRX statistics for the scanning process.

```
diagnose lldprx stats scan
```

diagnose log

log

This topic includes the following commands:

- [diagnose log alertmail on page 1673](#)
- [diagnose log alertmail authcode on page 1673](#)
- [diagnose log alertmail test on page 1673](#)
- [diagnose log check-empty on page 1673](#)
- [diagnose log clear-kernel-stats on page 1673](#)
- [diagnose log dummy-log on page 1674](#)
- [diagnose log dummy-log fill on page 1674](#)
- [diagnose log dummy-log remove on page 1674](#)
- [diagnose log field-enum on page 1674](#)
- [diagnose log field-list on page 1674](#)
- [diagnose log kernel-stats on page 1674](#)
- [diagnose log severity on page 1675](#)
- [diagnose log show on page 1675](#)
- [diagnose log stress-test on page 1675](#)
- [diagnose log sub-category on page 1675](#)
- [diagnose log test on page 1675](#)

- [diagnose log test-text on page 1675](#)

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 netlink

netlink

This topic includes the following commands:

- [diagnose netlink backlog on page 1676](#)
- [diagnose netlink backlog get on page 1676](#)
- [diagnose netlink backlog set on page 1677](#)
- [diagnose netlink brctl on page 1677](#)
- [diagnose netlink brctl forward-domain-status on page 1677](#)
- [diagnose netlink brctl interface-stats on page 1677](#)
- [diagnose netlink brctl list on page 1677](#)
- [diagnose netlink brctl name on page 1677](#)
- [diagnose netlink brctl vlan-filt-conf on page 1678](#)
- [diagnose netlink device on page 1678](#)
- [diagnose netlink device list on page 1678](#)
- [diagnose netlink interface on page 1678](#)
- [diagnose netlink interface clear on page 1678](#)
- [diagnose netlink interface list on page 1679](#)
- [diagnose netlink interface packet-rate on page 1679](#)
- [diagnose netlink interface speed-test on page 1679](#)
- [diagnose netlink interface speed-test-result on page 1679](#)
- [diagnose netlink interface speed-test-result-clear on page 1679](#)
- [diagnose netlink intf-class on page 1680](#)
- [diagnose netlink intf-class list on page 1680](#)
- [diagnose netlink intf-qdisc on page 1680](#)
- [diagnose netlink intf-qdisc list on page 1680](#)
- [diagnose netlink qlen on page 1680](#)
- [diagnose netlink qlen get on page 1681](#)
- [diagnose netlink qlen set on page 1681](#)

diagnose netlink backlog

UDP sockets.

```
diagnose netlink backlog
```

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

bridge

```
diagnose netlink brctl
```

diagnose netlink brctl forward-domain-status

forward-domain-status

```
diagnose netlink brctl forward-domain-status
```

diagnose netlink brctl interface-stats

interface-stats

```
diagnose netlink brctl interface-stats
```

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 brctl vlan-filt-conf

vlan-filt-conf

```
diagnose netlink brctl vlan-filt-conf
```

diagnose netlink device

devices

```
diagnose netlink device
```

diagnose netlink device list

List devices.

```
diagnose netlink device list
```

diagnose netlink interface

Network interfaces.

```
diagnose netlink interface
```

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 intf-class

Network interface class.

```
diagnose netlink intf-class
```

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.

```
diagnose netlink intf-qdisc
```

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.

```
diagnose netlink qlen
```

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 nodejs

Node.JS web server diagnostics.

This topic includes the following commands:

- [diagnose nodejs health-check on page 1682](#)
- [diagnose nodejs health-check ping on page 1682](#)
- [diagnose nodejs logs on page 1682](#)
- [diagnose nodejs logs delete on page 1682](#)
- [diagnose nodejs logs list on page 1682](#)
- [diagnose nodejs logs show on page 1682](#)
- [diagnose nodejs logs show-all on page 1683](#)
- [diagnose nodejs performance on page 1683](#)
- [diagnose nodejs performance mass-ztna-event-logs on page 1683](#)
- [diagnose nodejs process on page 1683](#)
- [diagnose nodejs process restart on page 1683](#)

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 <count>
```

Parameter	Description	Type	Size
<count>	Number of events to generate.	string	

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 1684](#)

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 1684](#)
- [diagnose on-demand-sniffer list on page 1685](#)
- [diagnose on-demand-sniffer start on page 1685](#)
- [diagnose on-demand-sniffer stop on page 1685](#)

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 preload

HTTP preload daemon

This topic includes the following commands:

- [diagnose preload clear on page 1686](#)
- [diagnose preload debug on page 1686](#)
- [diagnose preload log-show on page 1686](#)
- [diagnose preload restart on page 1686](#)
- [diagnose preload stats on page 1686](#)

diagnose preload clear

Restart daemon, reset statistics & remove scheduled tasks

```
diagnose preload clear
```

diagnose preload debug

Set debug level for deamon

```
diagnose preload debug <debug level>
```

Parameter	Description	Type	Size
<debug level>	Hexadecimal number	string	

diagnose preload log-show

Show log of daemon

```
diagnose preload log-show <log generation> <time format>
```

Parameter	Description	Type	Size
<log generation>	Log generation: default 0	string	
<time format>	Time format: 0 for human readable and 1 for raw, default 0	string	

diagnose preload restart

Restart the daemon and reset statistics

```
diagnose preload restart
```

diagnose preload stats

Show statistics.

```
diagnose preload stats
```

diagnose report

report

This topic includes the following commands:

- [diagnose report clear-filter on page 1687](#)
- [diagnose report dataset on page 1687](#)
- [diagnose report filter on page 1687](#)
- [diagnose report min-points on page 1687](#)
- [diagnose report ondemand-table on page 1688](#)
- [diagnose report sql on page 1688](#)
- [diagnose report time on page 1688](#)
- [diagnose report top-n on page 1688](#)

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 1688](#)
- [diagnose report-runner trigger on page 1689](#)
- [diagnose report-runner trigger security-rating-reports on page 1689](#)
- [diagnose report-runner vuln-clean on page 1689](#)
- [diagnose report-runner vuln-read on page 1689](#)

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 security-rating on page 1690](#)
- [diagnose report-runner-v2 security-rating clean on page 1690](#)
- [diagnose report-runner-v2 security-rating reset-trigger on page 1690](#)

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 saas

SaaS diagnose commands.

This topic includes the following commands:

- [diagnose saas reload on page 1690](#)
- [diagnose saas show on page 1690](#)
- [diagnose saas show apps on page 1691](#)
- [diagnose saas show details on page 1691](#)
- [diagnose saas show status on page 1691](#)

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 1691](#)
- [diagnose settings reset on page 1691](#)

diagnose settings info

Show all diagnose settings.

```
diagnose settings info
```

diagnose settings reset

Reset all diagnose settings.

```
diagnose settings reset
```

diagnose sniffer

Sniffer command.

This topic includes the following commands:

- [diagnose sniffer migsock on page 1692](#)
- [diagnose sniffer migsock debug-trace on page 1692](#)
- [diagnose sniffer migsock debug-trace disable on page 1692](#)
- [diagnose sniffer migsock debug-trace enable on page 1693](#)
- [diagnose sniffer migsock filter on page 1693](#)
- [diagnose sniffer migsock ssl-trace on page 1693](#)
- [diagnose sniffer migsock ssl-trace disable on page 1693](#)
- [diagnose sniffer migsock ssl-trace enable on page 1693](#)
- [diagnose sniffer migsock start on page 1693](#)
- [diagnose sniffer migsock timestamp on page 1694](#)
- [diagnose sniffer migsock timestamp disable on page 1694](#)
- [diagnose sniffer migsock timestamp enable on page 1694](#)
- [diagnose sniffer packet on page 1694](#)

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
```

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> <hostnames>
```



This command may cause high CPU and memory usage. To close, press Ctrl + C.

Parameter	Description	Type	Size
<interface>	Network interfaces 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	

Parameter	Description	Type	Size
<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	
<hostnames>	Hostnames to filter sniffed packets with.	string	

diagnose snmp

snmp

This topic includes the following commands:

- [diagnose snmp ip on page 1695](#)
- [diagnose snmp ip frags on page 1696](#)
- [diagnose snmp ip icmp on page 1696](#)
- [diagnose snmp ip tcp on page 1696](#)
- [diagnose snmp ip udp on page 1696](#)
- [diagnose snmp ip6 on page 1696](#)
- [diagnose snmp ip6 frags on page 1697](#)
- [diagnose snmp ip6 icmp6 on page 1697](#)
- [diagnose snmp ip6 udp6 on page 1697](#)
- [diagnose snmp net on page 1697](#)
- [diagnose snmp net stat on page 1697](#)
- [diagnose snmp trap on page 1698](#)
- [diagnose snmp trap send on page 1698](#)

diagnose snmp ip

Some IP stats.

```
diagnose snmp ip
```

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 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.

```
diagnose snmp ip6
```

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 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.

```
diagnose snmp net
```

diagnose snmp net stat

Network statistics.

```
diagnose snmp net stat
```

diagnose snmp trap

SNMP trap diagnostics.

```
diagnose snmp trap
```

diagnose snmp trap send

Generate a trap event.

```
diagnose snmp trap send
```

diagnose sys

system

This topic includes the following commands:

- [diagnose sys botnet-domain on page 1709](#)
- [diagnose sys botnet-domain hit on page 1709](#)
- [diagnose sys botnet-domain list on page 1710](#)
- [diagnose sys botnet-ip on page 1710](#)
- [diagnose sys botnet-ip find on page 1710](#)
- [diagnose sys botnet-ip flush on page 1710](#)
- [diagnose sys botnet-ip hit on page 1710](#)
- [diagnose sys botnet-ip list on page 1710](#)
- [diagnose sys cmdb on page 1711](#)
- [diagnose sys cmdb check-lock on page 1711](#)
- [diagnose sys cmdb dump on page 1711](#)
- [diagnose sys cmdb dump vdom on page 1711](#)
- [diagnose sys cmdb flag on page 1711](#)
- [diagnose sys cmdb flag info on page 1712](#)
- [diagnose sys cmdb flag reset on page 1712](#)
- [diagnose sys cmdb flag reset script-running on page 1712](#)
- [diagnose sys cmdb info on page 1712](#)
- [diagnose sys cmdb obj-verno on page 1712](#)
- [diagnose sys cmdb refcnt on page 1712](#)
- [diagnose sys cmdb refcnt reset on page 1713](#)

- [diagnose sys cmdb refcnt show on page 1713](#)
- [diagnose sys cmdb set-readlock on page 1713](#)
- [diagnose sys cmdb unset-readlock on page 1713](#)
- [diagnose sys cmdb-profile on page 1713](#)
- [diagnose sys cmdb-profile info on page 1714](#)
- [diagnose sys cmdb-profile node on page 1714](#)
- [diagnose sys cmdb-profile reset on page 1714](#)
- [diagnose sys cmdb-profile top10 on page 1714](#)
- [diagnose sys cmdb-profile top10 average on page 1714](#)
- [diagnose sys cmdb-profile top10 total on page 1715](#)
- [diagnose sys config-transaction on page 1715](#)
- [diagnose sys config-transaction show on page 1715](#)
- [diagnose sys config-transaction show entity-by-txn on page 1715](#)
- [diagnose sys config-transaction show mctx on page 1715](#)
- [diagnose sys config-transaction show txn-cli-commands on page 1716](#)
- [diagnose sys config-transaction show txn-entity on page 1716](#)
- [diagnose sys config-transaction show txn-info on page 1716](#)
- [diagnose sys config-transaction show txn-lock on page 1716](#)
- [diagnose sys config-transaction show txn-meta on page 1716](#)
- [diagnose sys config-transaction status on page 1716](#)
- [diagnose sys conntrack on page 1717](#)
- [diagnose sys conntrack clear on page 1717](#)
- [diagnose sys conntrack count on page 1717](#)
- [diagnose sys conntrack list-dying4 on page 1717](#)
- [diagnose sys conntrack list-dying6 on page 1717](#)
- [diagnose sys conntrack list-unconfirmed4 on page 1717](#)
- [diagnose sys conntrack list-unconfirmed6 on page 1718](#)
- [diagnose sys conntrack list4 on page 1718](#)
- [diagnose sys conntrack list6 on page 1718](#)
- [diagnose sys conntrack stats on page 1718](#)
- [diagnose sys csf on page 1718](#)
- [diagnose sys csf authorization on page 1718](#)
- [diagnose sys csf authorization accept on page 1719](#)
- [diagnose sys csf authorization deny on page 1719](#)
- [diagnose sys csf authorization pending-list on page 1719](#)
- [diagnose sys csf downstream on page 1719](#)
- [diagnose sys csf downstream-devices on page 1720](#)
- [diagnose sys csf dynamic-sync-read on page 1720](#)
- [diagnose sys csf dynamic-sync-request on page 1720](#)
- [diagnose sys csf dynamic-sync-update on page 1720](#)
- [diagnose sys csf fabric-device on page 1721](#)
- [diagnose sys csf fabric-device list on page 1721](#)
- [diagnose sys csf file on page 1721](#)

- [diagnose sys csf file cat on page 1721](#)
- [diagnose sys csf file top-mem on page 1721](#)
- [diagnose sys csf forticloud-id-list on page 1722](#)
- [diagnose sys csf get-bulk-global-view on page 1722](#)
- [diagnose sys csf global on page 1722](#)
- [diagnose sys csf initialize-cmd on page 1722](#)
- [diagnose sys csf license on page 1722](#)
- [diagnose sys csf merge-cmd on page 1723](#)
- [diagnose sys csf neighbor on page 1723](#)
- [diagnose sys csf neighbor flush on page 1723](#)
- [diagnose sys csf neighbor list on page 1723](#)
- [diagnose sys csf query on page 1724](#)
- [diagnose sys csf ratelimit-test-sender on page 1724](#)
- [diagnose sys csf ratelimit-test-server on page 1724](#)
- [diagnose sys csf send-test-log-upstream on page 1724](#)
- [diagnose sys csf seqpacket-message-listener on page 1725](#)
- [diagnose sys csf seqpacket-message-sender on page 1725](#)
- [diagnose sys csf stream-message-listener on page 1725](#)
- [diagnose sys csf stream-message-sender on page 1725](#)
- [diagnose sys csf tunnel-test-listener on page 1726](#)
- [diagnose sys csf tunnel-test-sender on page 1726](#)
- [diagnose sys csf upstream on page 1726](#)
- [diagnose sys csf versions on page 1726](#)
- [diagnose sys dayst-info on page 1726](#)
- [diagnose sys device on page 1727](#)
- [diagnose sys device add on page 1727](#)
- [diagnose sys device delete on page 1727](#)
- [diagnose sys device list on page 1727](#)
- [diagnose sys external-resource on page 1728](#)
- [diagnose sys external-resource list on page 1728](#)
- [diagnose sys external-resource push-add on page 1728](#)
- [diagnose sys external-resource push-api-json-commands on page 1728](#)
- [diagnose sys external-resource push-remove on page 1728](#)
- [diagnose sys external-resource push-snapshot on page 1729](#)
- [diagnose sys external-resource stats on page 1729](#)
- [diagnose sys fips on page 1729](#)
- [diagnose sys fips error-mode on page 1729](#)
- [diagnose sys fips kat-error on page 1729](#)
- [diagnose sys forticonverter on page 1730](#)
- [diagnose sys forticonverter available-source-devices on page 1730](#)
- [diagnose sys forticonverter create-ticket on page 1730](#)
- [diagnose sys forticonverter custom-create-ticket on page 1730](#)
- [diagnose sys forticonverter download-status on page 1730](#)

- [diagnose sys forticonverter eligibility-status on page 1731](#)
- [diagnose sys forticonverter get-prompt-visibility on page 1731](#)
- [diagnose sys forticonverter result-availability on page 1731](#)
- [diagnose sys forticonverter set-source-fortigate on page 1731](#)
- [diagnose sys forticonverter source-config-upload-status on page 1732](#)
- [diagnose sys forticonverter source-interfaces on page 1732](#)
- [diagnose sys forticonverter start-download on page 1732](#)
- [diagnose sys forticonverter submitted-info on page 1732](#)
- [diagnose sys forticonverter update-eligibility on page 1733](#)
- [diagnose sys forticonverter update-result-availability on page 1733](#)
- [diagnose sys forticonverter upload-local-config on page 1733](#)
- [diagnose sys forticonverter upload-status on page 1733](#)
- [diagnose sys ha on page 1733](#)
- [diagnose sys ha check-vc on page 1734](#)
- [diagnose sys ha checksum on page 1734](#)
- [diagnose sys ha checksum cached on page 1734](#)
- [diagnose sys ha checksum cluster on page 1734](#)
- [diagnose sys ha checksum log on page 1734](#)
- [diagnose sys ha checksum log clear on page 1734](#)
- [diagnose sys ha checksum log disable on page 1735](#)
- [diagnose sys ha checksum log enable on page 1735](#)
- [diagnose sys ha checksum recalculate on page 1735](#)
- [diagnose sys ha checksum show on page 1735](#)
- [diagnose sys ha checksum show-nonsync on page 1736](#)
- [diagnose sys ha checksum test on page 1736](#)
- [diagnose sys ha dump-by on page 1736](#)
- [diagnose sys ha dump-by debug-zone on page 1736](#)
- [diagnose sys ha dump-by device on page 1736](#)
- [diagnose sys ha dump-by group on page 1736](#)
- [diagnose sys ha dump-by kernel on page 1737](#)
- [diagnose sys ha dump-by rcache on page 1737](#)
- [diagnose sys ha dump-by vcluster on page 1737](#)
- [diagnose sys ha dump-by vdom on page 1737](#)
- [diagnose sys ha extfile-sig on page 1737](#)
- [diagnose sys ha fgsp-zone on page 1737](#)
- [diagnose sys ha fib on page 1738](#)
- [diagnose sys ha hactx-stats on page 1738](#)
- [diagnose sys ha hactx-stats clear on page 1738](#)
- [diagnose sys ha hadiff on page 1738](#)
- [diagnose sys ha hadiff log on page 1738](#)
- [diagnose sys ha hadiff log clear on page 1738](#)
- [diagnose sys ha hadiff log disable on page 1739](#)
- [diagnose sys ha hadiff log enable on page 1739](#)

- [diagnose sys ha hadiff max-sync-turns on page 1739](#)
- [diagnose sys ha hadiff max-unsync-wait on page 1739](#)
- [diagnose sys ha hadiff status on page 1739](#)
- [diagnose sys ha hadiff sync-from-higher on page 1740](#)
- [diagnose sys ha hasync-conn-max-buf on page 1740](#)
- [diagnose sys ha hasync-stats on page 1740](#)
- [diagnose sys ha hasync-stats all on page 1740](#)
- [diagnose sys ha hasync-stats by-object on page 1740](#)
- [diagnose sys ha hasync-stats most-recent on page 1741](#)
- [diagnose sys ha hasync-stats most-time on page 1741](#)
- [diagnose sys ha heartbeat on page 1741](#)
- [diagnose sys ha history on page 1741](#)
- [diagnose sys ha history clear on page 1741](#)
- [diagnose sys ha history read on page 1742](#)
- [diagnose sys ha mac on page 1742](#)
- [diagnose sys ha pingsvr-secondary-force-reset on page 1742](#)
- [diagnose sys ha recalculate-extfile-signature on page 1742](#)
- [diagnose sys ha reset-health-status on page 1742](#)
- [diagnose sys ha reset-uptime on page 1742](#)
- [diagnose sys ha reset-uptime-primary-only on page 1743](#)
- [diagnose sys ha session-sync-dev on page 1743](#)
- [diagnose sys ha session-sync-dev clear on page 1743](#)
- [diagnose sys ha session-sync-dev set on page 1743](#)
- [diagnose sys ha standalone-peers on page 1743](#)
- [diagnose sys ha standalone-peers reset-stats on page 1743](#)
- [diagnose sys ha stats on page 1744](#)
- [diagnose sys ha status on page 1744](#)
- [diagnose sys ha sync-stats on page 1744](#)
- [diagnose sys ha sync-stats-reset on page 1744](#)
- [diagnose sys ha vlan-hb-monitor on page 1744](#)
- [diagnose sys icap-remote-server on page 1744](#)
- [diagnose sys icap-remote-server status on page 1745](#)
- [diagnose sys iotop on page 1745](#)
- [diagnose sys link-monitor on page 1745](#)
- [diagnose sys link-monitor filter on page 1745](#)
- [diagnose sys link-monitor filter clear on page 1745](#)
- [diagnose sys link-monitor filter name on page 1745](#)
- [diagnose sys link-monitor interface on page 1746](#)
- [diagnose sys link-monitor launch on page 1746](#)
- [diagnose sys link-monitor reset-monitor on page 1746](#)
- [diagnose sys link-monitor sdwan-hc on page 1746](#)
- [diagnose sys link-monitor sdwan-service on page 1747](#)
- [diagnose sys link-monitor shm-band-stats on page 1747](#)

- [diagnose sys link-monitor shm-stats on page 1747](#)
- [diagnose sys link-monitor status on page 1747](#)
- [diagnose sys nmi-watchdog on page 1748](#)
- [diagnose sys nmi-watchdog disable on page 1748](#)
- [diagnose sys nmi-watchdog enable on page 1748](#)
- [diagnose sys nmi-watchdog reboot on page 1748](#)
- [diagnose sys nmi-watchdog reboot disable on page 1748](#)
- [diagnose sys nmi-watchdog reboot enable on page 1748](#)
- [diagnose sys nmi-watchdog threshold on page 1749](#)
- [diagnose sys ntp on page 1749](#)
- [diagnose sys ntp status on page 1749](#)
- [diagnose sys pair on page 1749](#)
- [diagnose sys process on page 1749](#)
- [diagnose sys process daemon-auto-restart on page 1749](#)
- [diagnose sys process dump on page 1750](#)
- [diagnose sys process nameof on page 1750](#)
- [diagnose sys process pidof on page 1750](#)
- [diagnose sys process pstack on page 1750](#)
- [diagnose sys process sock-mem on page 1751](#)
- [diagnose sys process socket on page 1751](#)
- [diagnose sys process trace on page 1751](#)
- [diagnose sys profile on page 1751](#)
- [diagnose sys profile cpumask on page 1751](#)
- [diagnose sys profile show on page 1752](#)
- [diagnose sys profile show detail on page 1752](#)
- [diagnose sys profile show order on page 1752](#)
- [diagnose sys profile start on page 1752](#)
- [diagnose sys profile step on page 1752](#)
- [diagnose sys profile stop on page 1752](#)
- [diagnose sys profile sysmap on page 1753](#)
- [diagnose sys ptp on page 1753](#)
- [diagnose sys ptp status on page 1753](#)
- [diagnose sys scanunit on page 1753](#)
- [diagnose sys scanunit auto-restart on page 1753](#)
- [diagnose sys scanunit auto-restart requests on page 1753](#)
- [diagnose sys scanunit auto-restart reset on page 1754](#)
- [diagnose sys scanunit auto-restart status on page 1754](#)
- [diagnose sys scanunit auto-restart time on page 1754](#)
- [diagnose sys scanunit av-filetype-reuse on page 1754](#)
- [diagnose sys scanunit av-filetype-reuse disable on page 1754](#)
- [diagnose sys scanunit av-filetype-reuse enable on page 1754](#)
- [diagnose sys scanunit bypass on page 1755](#)
- [diagnose sys scanunit bypass clear on page 1755](#)

- [diagnose sys scanunit bypass disable on page 1755](#)
- [diagnose sys scanunit bypass disable category on page 1755](#)
- [diagnose sys scanunit bypass disable category all on page 1755](#)
- [diagnose sys scanunit bypass disable category av-engine on page 1755](#)
- [diagnose sys scanunit bypass disable category scanunit on page 1756](#)
- [diagnose sys scanunit bypass disable protocol on page 1756](#)
- [diagnose sys scanunit bypass disable protocol all on page 1756](#)
- [diagnose sys scanunit bypass disable protocol cifs on page 1756](#)
- [diagnose sys scanunit bypass disable protocol ftp on page 1756](#)
- [diagnose sys scanunit bypass disable protocol http on page 1756](#)
- [diagnose sys scanunit bypass disable protocol imap on page 1757](#)
- [diagnose sys scanunit bypass disable protocol nntp on page 1757](#)
- [diagnose sys scanunit bypass disable protocol pop3 on page 1757](#)
- [diagnose sys scanunit bypass disable protocol smtp on page 1757](#)
- [diagnose sys scanunit bypass enable on page 1757](#)
- [diagnose sys scanunit bypass enable category on page 1757](#)
- [diagnose sys scanunit bypass enable category all on page 1758](#)
- [diagnose sys scanunit bypass enable category av-engine on page 1758](#)
- [diagnose sys scanunit bypass enable category scanunit on page 1758](#)
- [diagnose sys scanunit bypass enable protocol on page 1758](#)
- [diagnose sys scanunit bypass enable protocol all on page 1758](#)
- [diagnose sys scanunit bypass enable protocol cifs on page 1758](#)
- [diagnose sys scanunit bypass enable protocol ftp on page 1759](#)
- [diagnose sys scanunit bypass enable protocol http on page 1759](#)
- [diagnose sys scanunit bypass enable protocol imap on page 1759](#)
- [diagnose sys scanunit bypass enable protocol nntp on page 1759](#)
- [diagnose sys scanunit bypass enable protocol pop3 on page 1759](#)
- [diagnose sys scanunit bypass enable protocol smtp on page 1759](#)
- [diagnose sys scanunit bypass show on page 1760](#)
- [diagnose sys scanunit cfg on page 1760](#)
- [diagnose sys scanunit cfg clear on page 1760](#)
- [diagnose sys scanunit cfg list on page 1760](#)
- [diagnose sys scanunit crash-dump on page 1760](#)
- [diagnose sys scanunit crash-dump clear on page 1760](#)
- [diagnose sys scanunit crash-dump disable on page 1761](#)
- [diagnose sys scanunit crash-dump enable on page 1761](#)
- [diagnose sys scanunit crash-dump read on page 1761](#)
- [diagnose sys scanunit debug on page 1761](#)
- [diagnose sys scanunit debug all on page 1761](#)
- [diagnose sys scanunit debug analytics on page 1761](#)
- [diagnose sys scanunit debug antisipam on page 1762](#)
- [diagnose sys scanunit debug daemon on page 1762](#)
- [diagnose sys scanunit debug dlp on page 1762](#)

- [diagnose sys scanunit debug file-filter on page 1762](#)
- [diagnose sys scanunit debug ia on page 1763](#)
- [diagnose sys scanunit debug icb on page 1763](#)
- [diagnose sys scanunit debug job on page 1763](#)
- [diagnose sys scanunit debug level on page 1763](#)
- [diagnose sys scanunit debug level error on page 1763](#)
- [diagnose sys scanunit debug level info on page 1764](#)
- [diagnose sys scanunit debug level verbose on page 1764](#)
- [diagnose sys scanunit debug level warning on page 1764](#)
- [diagnose sys scanunit debug outbreak-prevention on page 1764](#)
- [diagnose sys scanunit debug quarantine on page 1764](#)
- [diagnose sys scanunit debug reset on page 1765](#)
- [diagnose sys scanunit debug sane on page 1765](#)
- [diagnose sys scanunit debug show on page 1765](#)
- [diagnose sys scanunit dlp on page 1765](#)
- [diagnose sys scanunit dlp reset on page 1765](#)
- [diagnose sys scanunit dlp status on page 1765](#)
- [diagnose sys scanunit dlp threshold on page 1766](#)
- [diagnose sys scanunit file-hash on page 1766](#)
- [diagnose sys scanunit file-hash list on page 1766](#)
- [diagnose sys scanunit file-hash list all on page 1766](#)
- [diagnose sys scanunit file-hash list md5 on page 1766](#)
- [diagnose sys scanunit file-hash list sha1 on page 1766](#)
- [diagnose sys scanunit file-hash list sha256 on page 1767](#)
- [diagnose sys scanunit file-hash query on page 1767](#)
- [diagnose sys scanunit file-hash query md5 on page 1767](#)
- [diagnose sys scanunit file-hash query sha1 on page 1767](#)
- [diagnose sys scanunit file-hash query sha256 on page 1767](#)
- [diagnose sys scanunit file-hash status on page 1768](#)
- [diagnose sys scanunit filter on page 1768](#)
- [diagnose sys scanunit filter clear on page 1768](#)
- [diagnose sys scanunit filter list on page 1768](#)
- [diagnose sys scanunit filter negate on page 1768](#)
- [diagnose sys scanunit filter negate vd on page 1768](#)
- [diagnose sys scanunit filter negate worker on page 1769](#)
- [diagnose sys scanunit filter vd on page 1769](#)
- [diagnose sys scanunit filter worker on page 1769](#)
- [diagnose sys scanunit log on page 1769](#)
- [diagnose sys scanunit log filter on page 1769](#)
- [diagnose sys scanunit log filter clear on page 1770](#)
- [diagnose sys scanunit log filter list on page 1770](#)
- [diagnose sys scanunit log filter negate on page 1770](#)
- [diagnose sys scanunit log filter negate vd on page 1770](#)

- [diagnose sys scanunit log filter negate worker on page 1770](#)
- [diagnose sys scanunit log filter vd on page 1770](#)
- [diagnose sys scanunit log filter worker on page 1771](#)
- [diagnose sys scanunit memory on page 1771](#)
- [diagnose sys scanunit memory conserve on page 1771](#)
- [diagnose sys scanunit memory conserve enter on page 1771](#)
- [diagnose sys scanunit memory conserve exit on page 1771](#)
- [diagnose sys scanunit reload-avdb on page 1771](#)
- [diagnose sys scanunit reload-aveng on page 1772](#)
- [diagnose sys scanunit reload-fsa-ext on page 1772](#)
- [diagnose sys scanunit restart on page 1772](#)
- [diagnose sys scanunit simulate-crash on page 1772](#)
- [diagnose sys scanunit simulate-crash lockup-workers on page 1772](#)
- [diagnose sys scanunit simulate-crash lockup-workers all on page 1772](#)
- [diagnose sys scanunit simulate-crash lockup-workers worker on page 1773](#)
- [diagnose sys scanunit simulate-error on page 1773](#)
- [diagnose sys scanunit simulate-error av-engine-delay on page 1773](#)
- [diagnose sys scanunit simulate-error av-error on page 1773](#)
- [diagnose sys scanunit simulate-error av-status on page 1773](#)
- [diagnose sys scanunit simulate-error cdr-error on page 1774](#)
- [diagnose sys scanunit simulate-error reset on page 1774](#)
- [diagnose sys scanunit simulate-error scan-error-code on page 1774](#)
- [diagnose sys scanunit simulate-error status on page 1774](#)
- [diagnose sys scanunit stats on page 1774](#)
- [diagnose sys scanunit stats all on page 1775](#)
- [diagnose sys scanunit stats clear on page 1775](#)
- [diagnose sys scanunit stats crash on page 1775](#)
- [diagnose sys scanunit stats forker on page 1775](#)
- [diagnose sys scanunit stats list on page 1775](#)
- [diagnose sys scanunit stats manager on page 1775](#)
- [diagnose sys scanunit stats worker on page 1776](#)
- [diagnose sys scanunit valgrind on page 1776](#)
- [diagnose sys scanunit valgrind disable on page 1776](#)
- [diagnose sys scanunit valgrind enable on page 1776](#)
- [diagnose sys scanunit valgrind log on page 1776](#)
- [diagnose sys scanunit valgrind log clear on page 1776](#)
- [diagnose sys scanunit valgrind log show on page 1777](#)
- [diagnose sys scanunit valgrind memcheck on page 1777](#)
- [diagnose sys scanunit valgrind memcheck_less on page 1777](#)
- [diagnose sys scanunit valgrind status on page 1777](#)
- [diagnose sys scanunit vdom-stats on page 1777](#)
- [diagnose sys scanunit vdom-stats all on page 1777](#)
- [diagnose sys scanunit vdom-stats clear on page 1778](#)

- [diagnose sys scanunit vdom-stats clear-all on page 1778](#)
- [diagnose sys scanunit vdom-stats list on page 1778](#)
- [diagnose sys scanunit watchdog-override on page 1778](#)
- [diagnose sys scanunit watchdog-override disable on page 1778](#)
- [diagnose sys scanunit watchdog-override enable on page 1778](#)
- [diagnose sys scanunit watchdog-override interval on page 1779](#)
- [diagnose sys sdn on page 1779](#)
- [diagnose sys sdn cache on page 1779](#)
- [diagnose sys sdn status on page 1779](#)
- [diagnose sys server-probe on page 1780](#)
- [diagnose sys server-probe response on page 1780](#)
- [diagnose sys session on page 1780](#)
- [diagnose sys session clear on page 1780](#)
- [diagnose sys session count on page 1780](#)
- [diagnose sys session exp-stat on page 1780](#)
- [diagnose sys session expectation on page 1781](#)
- [diagnose sys session filter on page 1781](#)
- [diagnose sys session filter clear on page 1781](#)
- [diagnose sys session filter clear dintf on page 1781](#)
- [diagnose sys session filter clear dport on page 1781](#)
- [diagnose sys session filter clear dst on page 1781](#)
- [diagnose sys session filter clear nsrc on page 1782](#)
- [diagnose sys session filter clear policy on page 1782](#)
- [diagnose sys session filter clear proto on page 1782](#)
- [diagnose sys session filter clear proto-state on page 1782](#)
- [diagnose sys session filter clear sintf on page 1782](#)
- [diagnose sys session filter clear sport on page 1782](#)
- [diagnose sys session filter clear src on page 1783](#)
- [diagnose sys session filter dintf on page 1783](#)
- [diagnose sys session filter dport on page 1783](#)
- [diagnose sys session filter dst on page 1783](#)
- [diagnose sys session filter nsrc on page 1783](#)
- [diagnose sys session filter policy on page 1784](#)
- [diagnose sys session filter proto on page 1784](#)
- [diagnose sys session filter sintf on page 1784](#)
- [diagnose sys session filter sport on page 1784](#)
- [diagnose sys session filter src on page 1785](#)
- [diagnose sys session full-stat on page 1785](#)
- [diagnose sys session list on page 1785](#)
- [diagnose sys session stat on page 1785](#)
- [diagnose sys session ttl on page 1785](#)
- [diagnose sys session6 on page 1785](#)
- [diagnose sys session6 clear on page 1786](#)

- [diagnose sys session6 expectation on page 1786](#)
- [diagnose sys session6 filter on page 1786](#)
- [diagnose sys session6 filter clear on page 1786](#)
- [diagnose sys session6 filter clear dintf on page 1786](#)
- [diagnose sys session6 filter clear dport on page 1786](#)
- [diagnose sys session6 filter clear dst on page 1787](#)
- [diagnose sys session6 filter clear nsrc on page 1787](#)
- [diagnose sys session6 filter clear policy on page 1787](#)
- [diagnose sys session6 filter clear proto on page 1787](#)
- [diagnose sys session6 filter clear proto-state on page 1787](#)
- [diagnose sys session6 filter clear sintf on page 1787](#)
- [diagnose sys session6 filter clear sport on page 1788](#)
- [diagnose sys session6 filter clear src on page 1788](#)
- [diagnose sys session6 filter clear vd on page 1788](#)
- [diagnose sys session6 filter dintf on page 1788](#)
- [diagnose sys session6 filter dport on page 1788](#)
- [diagnose sys session6 filter dst on page 1789](#)
- [diagnose sys session6 filter nsrc on page 1789](#)
- [diagnose sys session6 filter policy on page 1789](#)
- [diagnose sys session6 filter proto on page 1789](#)
- [diagnose sys session6 filter sintf on page 1789](#)
- [diagnose sys session6 filter sport on page 1790](#)
- [diagnose sys session6 filter src on page 1790](#)
- [diagnose sys session6 list on page 1790](#)
- [diagnose sys shmfile on page 1790](#)
- [diagnose sys shmfile dump on page 1790](#)
- [diagnose sys shmfile dump oid-app on page 1791](#)
- [diagnose sys shmfile dump oid-slab on page 1791](#)
- [diagnose sys shmfile dump slab-file on page 1791](#)
- [diagnose sys shmfile dump table-count on page 1791](#)
- [diagnose sys shmfile dump table-count total on page 1791](#)
- [diagnose sys shmfile dump table-count vdom on page 1792](#)
- [diagnose sys shmfile dump vdom on page 1792](#)
- [diagnose sys tcp-option on page 1792](#)
- [diagnose sys tcp-option disable on page 1792](#)
- [diagnose sys tcp-option dump on page 1793](#)
- [diagnose sys tcp-option enable on page 1793](#)
- [diagnose sys tcpsock on page 1793](#)
- [diagnose sys tcpsock6 on page 1793](#)
- [diagnose sys top on page 1793](#)
- [diagnose sys top-all on page 1794](#)
- [diagnose sys top-fd on page 1794](#)
- [diagnose sys top-fd detail on page 1794](#)

- [diagnose sys top-mem on page 1794](#)
- [diagnose sys top-mem detail on page 1795](#)
- [diagnose sys top-sockmem on page 1795](#)
- [diagnose sys traffic on page 1795](#)
- [diagnose sys traffic app-stats on page 1795](#)
- [diagnose sys traffic app-stats list on page 1796](#)
- [diagnose sys udpsock on page 1796](#)
- [diagnose sys udpsock6 on page 1796](#)
- [diagnose sys uuid on page 1796](#)
- [diagnose sys uuid allow-manual-set on page 1796](#)
- [diagnose sys uuid allow-manual-set disable on page 1796](#)
- [diagnose sys uuid allow-manual-set enable on page 1797](#)
- [diagnose sys uuid generate on page 1797](#)
- [diagnose sys var-zone on page 1797](#)
- [diagnose sys var-zone show on page 1797](#)
- [diagnose sys vd on page 1797](#)
- [diagnose sys vd add on page 1797](#)
- [diagnose sys vd delete on page 1798](#)
- [diagnose sys vd list on page 1798](#)
- [diagnose sys vd set on page 1798](#)
- [diagnose sys vd stats on page 1798](#)
- [diagnose sys vlan on page 1798](#)
- [diagnose sys vlan list on page 1799](#)
- [diagnose sys vxlan on page 1799](#)
- [diagnose sys vxlan device on page 1799](#)
- [diagnose sys vxlan fdb on page 1799](#)
- [diagnose sys vxlan fdb list on page 1799](#)

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	
<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 cmdb

CMDB related information.

```
diagnose sys cmdb
```

diagnose sys cmdb check-lock

Check CMDB lock.

```
diagnose sys cmdb check-lock
```

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 conntrack

conntrack diagnostics.

```
diagnose sys conntrack
```

diagnose sys conntrack clear

Clear all conntrack.

```
diagnose sys conntrack clear
```

diagnose sys conntrack count

Show number of conntrack.

```
diagnose sys conntrack count
```

diagnose sys conntrack list-dying4

List IPv4 dying conntrack.

```
diagnose sys conntrack list-dying4
```

diagnose sys conntrack list-dying6

List IPv6 dying conntrack.

```
diagnose sys conntrack list-dying6
```

diagnose sys conntrack list-unconfirmed4

List IPv4 unconfirmed conntrack.

```
diagnose sys conntrack list-unconfirmed4
```

diagnose sys conntrack list-unconfirmed6

List IPv6 unconfirmed conntrack.

```
diagnose sys conntrack list-unconfirmed6
```

diagnose sys conntrack list4

List IPv4 conntrack.

```
diagnose sys conntrack list4
```

diagnose sys conntrack list6

List IPv6 conntrack.

```
diagnose sys conntrack list6
```

diagnose sys conntrack stats

Show conntrack statistics.

```
diagnose sys conntrack stats
```

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 FortiProxies.

```
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>
```

Parameter	Description	Type	Size
<content>	New data content string	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 license

Show a summary of FPX license sharing in the cluster.

```
diagnose sys csf license
```

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> [-p]
```

Parameter	Description	Type	Size
<path>	FGT1(SN):FGT2(SN):...:FGTn(SN)	string	
[-p]	partial process.	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 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 FortiProxies.

```
diagnose sys csf upstream
```

diagnose sys csf versions

get latest incremental version of CSF groups.

```
diagnose sys csf versions
```

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 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 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 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 ha

High availability.

```
diagnose sys ha
```

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 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 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 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 nmi-watchdog

nmi-watchdog

```
diagnose sys nmi-watchdog
```

diagnose sys nmi-watchdog disable

Disable NMI watchdog.

```
diagnose sys nmi-watchdog disable
```

diagnose sys nmi-watchdog enable

Enable NMI watchdog.

```
diagnose sys nmi-watchdog enable
```

diagnose sys nmi-watchdog reboot

reboot on lockup detection.

```
diagnose sys nmi-watchdog reboot
```

diagnose sys nmi-watchdog reboot disable

Disable reboot on lockup detection.

```
diagnose sys nmi-watchdog reboot disable
```

diagnose sys nmi-watchdog reboot enable

Enable reboot on lockup detection.

```
diagnose sys nmi-watchdog reboot enable
```


diagnose sys nmi-watchdog threshold

Duration of lockup that register as a detection.

```
diagnose sys nmi-watchdog threshold <seconds>
```

Parameter	Description	Type	Size
<seconds>	(6 to 40 seconds)	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 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 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 ptp

PTP daemon command.

```
diagnose sys ptp
```

diagnose sys ptp status

List PTP information.

```
diagnose sys ptp status
```

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-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 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 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 ia

Enable IA category.

```
diagnose sys scanunit debug ia <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 dlp

DLP data size scanning threshold settings.

```
diagnose sys scanunit dlp
```

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 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 reload-avdb

Reload AVDB.

```
diagnose sys scanunit reload-avdb
```

diagnose sys scanunit reload-aveng

Reload AV engine.

```
diagnose sys scanunit reload-aveng
```

diagnose sys scanunit reload-fsa-ext

Reload FSA extensions list.

```
diagnose sys scanunit reload-fsa-ext
```

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 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 forker

scanunit forker statistics.

```
diagnose sys scanunit stats forker
```

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 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 server-probe

Server probe.

```
diagnose sys server-probe
```

diagnose sys server-probe response

Probe response.

```
diagnose sys server-probe response
```

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 count

Show number of sessions.

```
diagnose sys session count
```

diagnose sys session exp-stat

Expectation session statistics.

```
diagnose sys session exp-stat
```


diagnose sys session expectation

List expectation session.

```
diagnose sys session expectation
```

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 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 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 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>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	

diagnose sys session filter dst

Destination IP address.

```
diagnose sys session filter dst <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	

diagnose sys session filter nsrc

NAT'd source ip address

```
diagnose sys session filter nsrc <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	NAT'd source ip (from)	string	

diagnose sys session filter policy

Policy ID.

```
diagnose sys session filter policy <xxx>
```

Parameter	Description	Type	Size
<xxx>	Policy ID (from).	string	

diagnose sys session filter proto

Protocol number.

```
diagnose sys session filter proto <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255>.	string	

diagnose sys session filter intf

Source interface.

```
diagnose sys session filter intf <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	Interface name.	string	

diagnose sys session filter sport

Source port.

```
diagnose sys session filter sport <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	

diagnose sys session filter src

Source IP address.

```
diagnose sys session filter src <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	string	

diagnose sys session full-stat

Fully stat session.

```
diagnose sys session full-stat
```

diagnose sys session list

List session.

```
diagnose sys session list
```

diagnose sys session stat

Stat session.

```
diagnose sys session stat
```

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 expectation

List IPv6 expectation session.

```
diagnose sys session6 expectation
```

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 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 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>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	

diagnose sys session6 filter dst

Destination IP address.

```
diagnose sys session6 filter dst <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Destination IP (from).	string	

diagnose sys session6 filter nsrc

NAT'd source IP address.

```
diagnose sys session6 filter nsrc <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	NAT'd source IP (from).	string	

diagnose sys session6 filter policy

Policy ID.

```
diagnose sys session6 filter policy <xxx>
```

Parameter	Description	Type	Size
<xxx>	Policy ID (from).	string	

diagnose sys session6 filter proto

Protocol number.

```
diagnose sys session6 filter proto <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255>.	string	

diagnose sys session6 filter intf

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>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	

diagnose sys session6 filter src

Source IP address.

```
diagnose sys session6 filter src <xxx:xxx::xxx:xxx>
```

Parameter	Description	Type	Size
<xxx:xxx::xxx:xxx>	Source IP (from).	string	

diagnose sys session6 list

List IPv6 session.

```
diagnose sys session6 list
```

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-id]
```

Parameter	Description	Type	Size
[file-id]	file id.	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 tcp-option

Enable/disable TCP option.

```
diagnose sys tcp-option
```

diagnose sys tcp-option disable

disable

```
diagnose sys tcp-option disable
```

diagnose sys tcp-option dump

Show TCP option status

```
diagnose sys tcp-option dump
```

diagnose sys tcp-option enable

enable

```
diagnose sys tcp-option 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 list

List traffic application statistics entry.

```
diagnose sys traffic app-stats list
```

diagnose sys udpsock

UDP sock info.

```
diagnose sys udpsock
```

diagnose sys udpsock6

UDP sock6 info.

```
diagnose sys udpsock6
```

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 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 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 test analytics-pdf-report

Retrieve analytics PDF report from FortiSandbox.

This topic includes the following commands:

- [diagnose test analytics-pdf-report list on page 1800](#)
- [diagnose test analytics-pdf-report max on page 1800](#)
- [diagnose test analytics-pdf-report request on page 1800](#)
- [diagnose test analytics-pdf-report status on page 1800](#)

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 1801](#)

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 1803](#)
- [diagnose test application acsd on page 1803](#)
- [diagnose test application autod on page 1803](#)
- [diagnose test application awsd on page 1803](#)
- [diagnose test application azd on page 1804](#)
- [diagnose test application bfd on page 1804](#)
- [diagnose test application cloudapid on page 1804](#)
- [diagnose test application cmdbsvr on page 1804](#)
- [diagnose test application csfd on page 1805](#)
- [diagnose test application ddnsd on page 1805](#)
- [diagnose test application dhcp6c on page 1805](#)
- [diagnose test application dhcp6r on page 1805](#)
- [diagnose test application dhcprelay on page 1805](#)
- [diagnose test application dlpfingerprint on page 1806](#)
- [diagnose test application dlpfpcache on page 1806](#)
- [diagnose test application dnsproxy on page 1806](#)
- [diagnose test application dsd on page 1806](#)
- [diagnose test application eap_supp on page 1807](#)
- [diagnose test application evpn on page 1807](#)
- [diagnose test application fas on page 1807](#)
- [diagnose test application fcnacd on page 1807](#)
- [diagnose test application fds_notify on page 1808](#)
- [diagnose test application fgtlogd on page 1808](#)
- [diagnose test application fnbamd on page 1808](#)
- [diagnose test application forticldd on page 1808](#)
- [diagnose test application forticron on page 1808](#)
- [diagnose test application fsd on page 1809](#)
- [diagnose test application fsvrd on page 1809](#)
- [diagnose test application gcpcd on page 1809](#)
- [diagnose test application harelay on page 1809](#)

- [diagnose test application hasync on page 1810](#)
- [diagnose test application hataalk on page 1810](#)
- [diagnose test application ibmd on page 1810](#)
- [diagnose test application imap on page 1810](#)
- [diagnose test application init on page 1811](#)
- [diagnose test application iotd on page 1811](#)
- [diagnose test application ipamd on page 1811](#)
- [diagnose test application ipamsd on page 1811](#)
- [diagnose test application ipldbd on page 1811](#)
- [diagnose test application ipsengine on page 1812](#)
- [diagnose test application ipsmonitor on page 1812](#)
- [diagnose test application ipsufd on page 1812](#)
- [diagnose test application kmipd on page 1812](#)
- [diagnose test application kubed on page 1813](#)
- [diagnose test application l2tpcd on page 1813](#)
- [diagnose test application lnkmttd on page 1813](#)
- [diagnose test application locallogd on page 1813](#)
- [diagnose test application miglogd on page 1814](#)
- [diagnose test application mrd on page 1814](#)
- [diagnose test application netxd on page 1814](#)
- [diagnose test application nntp on page 1814](#)
- [diagnose test application ocid on page 1814](#)
- [diagnose test application openstackd on page 1815](#)
- [diagnose test application ovrd on page 1815](#)
- [diagnose test application pcpd on page 1815](#)
- [diagnose test application pop3 on page 1815](#)
- [diagnose test application pptpcd on page 1816](#)
- [diagnose test application quarantined on page 1816](#)
- [diagnose test application radius-das on page 1816](#)
- [diagnose test application radiusd on page 1816](#)
- [diagnose test application radvd on page 1817](#)
- [diagnose test application reportd on page 1817](#)
- [diagnose test application sdncd on page 1817](#)
- [diagnose test application sdnd on page 1817](#)
- [diagnose test application sepmd on page 1817](#)
- [diagnose test application sessionsync on page 1818](#)
- [diagnose test application sfupgraded on page 1818](#)
- [diagnose test application smtp on page 1818](#)
- [diagnose test application snmpd on page 1818](#)
- [diagnose test application syslogd on page 1819](#)
- [diagnose test application updated on page 1819](#)
- [diagnose test application uploadd on page 1819](#)
- [diagnose test application urlfilter on page 1819](#)

- [diagnose test application vned on page 1820](#)
- [diagnose test application wad on page 1820](#)
- [diagnose test application wccpd on page 1820](#)
- [diagnose test application wf_monitor on page 1820](#)
- [diagnose test application wiredapd on page 1820](#)

diagnose test application acd

Aggregate Controller.

```
diagnose test application acd <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>
```

Parameter	Description	Type	Size
<Integer>	Test level.	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>
```

Parameter	Description	Type	Size
<Integer>	Test level.	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 fsd

FortiExplorer daemon.

```
diagnose test application fsd <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 hatalk

HA talk daemon.

```
diagnose test application hatalk <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>
```

Parameter	Description	Type	Size
<Integer>	Test level.	string	

diagnose test application miglogd

Miglog logging daemon.

```
diagnose test application miglogd <Integer>
```

Parameter	Description	Type	Size
<Integer>	Test level.	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>
```

Parameter	Description	Type	Size
<Integer>	Test level.	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 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>
```

Parameter	Description	Type	Size
<Integer>	Test level.	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>
```

Parameter	Description	Type	Size
<Integer>	Test level.	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 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 authserver

Test authentication server.

This topic includes the following commands:

- [diagnose test authserver cert on page 1821](#)
- [diagnose test authserver ext-idp on page 1821](#)
- [diagnose test authserver ldap on page 1822](#)
- [diagnose test authserver ldap-digest on page 1822](#)
- [diagnose test authserver ldap-direct on page 1822](#)
- [diagnose test authserver ldap-search on page 1822](#)
- [diagnose test authserver local on page 1822](#)
- [diagnose test authserver pop3 on page 1822](#)
- [diagnose test authserver radius on page 1823](#)
- [diagnose test authserver radius-direct on page 1823](#)
- [diagnose test authserver tacacs+ on page 1823](#)
- [diagnose test authserver tacacs+-direct on page 1823](#)
- [diagnose test authserver user on page 1823](#)

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+
```

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 1824](#)
- [diagnose test guest del on page 1824](#)
- [diagnose test guest list on page 1824](#)

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 security

System security test.

This topic includes the following commands:

- [diagnose test security mount-invalid-flag on page 1824](#)
- [diagnose test security status on page 1824](#)

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 1825](#)
- [diagnose test update tzdb on page 1825](#)

diagnose test update info

Display debug info.

```
diagnose test update info
```

diagnose test update tzdb

Test TZDB.

```
diagnose test update tzdb
```

diagnose tpm

TPM chip diagnostic feature

This topic includes the following commands:

- [diagnose tpm SHA-1 on page 1825](#)
- [diagnose tpm SHA-256 on page 1826](#)
- [diagnose tpm generate-random-number on page 1826](#)
- [diagnose tpm get-property on page 1826](#)
- [diagnose tpm get-var-property on page 1826](#)
- [diagnose tpm read-clock on page 1826](#)
- [diagnose tpm selftest on page 1827](#)
- [diagnose tpm shutdown-prepare on page 1827](#)

diagnose tpm SHA-1

HASH a sequence of num with SHA-1 algo

```
diagnose tpm SHA-1 <Byte Sequence>
```

Parameter	Description	Type	Size
<Byte Sequence>	Enter a byte sequence like '0F56FE...' for {0x0f, 0x56, 0xfe, ...}	string	

diagnose tpm SHA-256

HASH a sequence of num with SHA-256 algo

```
diagnose tpm SHA-256 <Byte Sequence>
```

Parameter	Description	Type	Size
<Byte Sequence>	Enter a byte sequence like '0F56FE...' for {0x0f, 0x56, 0xfe, ...}	string	

diagnose tpm generate-random-number

Generate a 4-byte random number

```
diagnose tpm generate-random-number
```

diagnose tpm get-property

Get TPM properties.

```
diagnose tpm get-property
```

diagnose tpm get-var-property

Get TPM var properties.

```
diagnose tpm get-var-property
```

diagnose tpm read-clock

Read TPM internal clock.

```
diagnose tpm read-clock
```

diagnose tpm selftest

Perform self tests.

```
diagnose tpm selftest
```

diagnose tpm shutdown-prepare

Prepare for TPM power cycle.

```
diagnose tpm shutdown-prepare
```

diagnose traffictest

Offloading traffic test using internal TX/RX

This topic includes the following commands:

- [diagnose traffictest client-intf on page 1827](#)
- [diagnose traffictest port on page 1827](#)
- [diagnose traffictest proto on page 1828](#)
- [diagnose traffictest proto 0 on page 1828](#)
- [diagnose traffictest proto 1 on page 1828](#)
- [diagnose traffictest run on page 1828](#)
- [diagnose traffictest server-intf on page 1828](#)
- [diagnose traffictest show on page 1829](#)

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]
```

Parameter	Description	Type	Size
[-h/arg]	Help/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 1830](#)
- [diagnose user banned-ip add on page 1830](#)
- [diagnose user banned-ip add src4 on page 1830](#)
- [diagnose user banned-ip add src6 on page 1831](#)
- [diagnose user banned-ip clear on page 1831](#)
- [diagnose user banned-ip delete on page 1831](#)
- [diagnose user banned-ip delete src4 on page 1831](#)
- [diagnose user banned-ip delete src6 on page 1831](#)
- [diagnose user banned-ip list on page 1832](#)
- [diagnose user banned-ip list all on page 1832](#)
- [diagnose user banned-ip list src4 on page 1832](#)
- [diagnose user banned-ip list src6 on page 1832](#)
- [diagnose user banned-ip stat on page 1832](#)
- [diagnose user banned-ip stress-test on page 1832](#)
- [diagnose user device on page 1833](#)
- [diagnose user device clear on page 1833](#)
- [diagnose user device del on page 1833](#)
- [diagnose user device filter on page 1833](#)
- [diagnose user device filter addr on page 1833](#)
- [diagnose user device filter clear on page 1834](#)
- [diagnose user device filter clear addr on page 1834](#)
- [diagnose user device filter clear generation on page 1834](#)
- [diagnose user device filter clear index on page 1834](#)
- [diagnose user device filter clear joined on page 1834](#)
- [diagnose user device filter clear vd on page 1835](#)

- [diagnose user device filter generation on page 1835](#)
- [diagnose user device filter joined on page 1835](#)
- [diagnose user device filter list on page 1835](#)
- [diagnose user device filter negate on page 1835](#)
- [diagnose user device filter negate addr on page 1836](#)
- [diagnose user device filter negate generation on page 1836](#)
- [diagnose user device filter negate index on page 1836](#)
- [diagnose user device filter negate joined on page 1836](#)
- [diagnose user device filter negate vd on page 1836](#)
- [diagnose user device filter vd on page 1836](#)
- [diagnose user device get on page 1837](#)
- [diagnose user device list on page 1837](#)
- [diagnose user device stats on page 1837](#)

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 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 filter

Filter for various src-vis diagnostics.

```
diagnose user device filter
```

diagnose user device filter addr

IPv4 address range.

```
diagnose user device filter addr <from> <to>
```

Parameter	Description	Type	Size
<from>	IPv4 address range.	string	
<to>	IPv4 address range.	string	

diagnose user device filter clear

Clear the filter or parameter.

```
diagnose user device filter clear
```

diagnose user device filter clear addr

Clear parameter.

```
diagnose user device filter clear addr
```

diagnose user device filter clear generation

Clear parameter.

```
diagnose user device filter clear generation
```

diagnose user device filter clear index

Clear parameter.

```
diagnose user device filter clear index
```

diagnose user device filter clear joined

Clear parameter.

```
diagnose user device filter clear joined
```

diagnose user device filter clear vd

Clear parameter.

```
diagnose user device filter clear vd
```

diagnose user device filter generation

Device generation.

```
diagnose user device filter generation <from> <to>
```

Parameter	Description	Type	Size
<from>	<from>	string	
<to>	<to>	string	

diagnose user device filter joined

Device is joined to another.

```
diagnose user device filter joined <value>
```

Parameter	Description	Type	Size
<value>	<value>	string	

diagnose user device filter list

Display the current filter.

```
diagnose user device filter list
```

diagnose user device filter negate

Negate the specified filter parameter.

```
diagnose user device filter negate
```

diagnose user device filter negate addr

Negate parameter.

```
diagnose user device filter negate addr
```

diagnose user device filter negate generation

Negate parameter.

```
diagnose user device filter negate generation
```

diagnose user device filter negate index

Negate parameter.

```
diagnose user device filter negate index
```

diagnose user device filter negate joined

Negate parameter.

```
diagnose user device filter negate joined
```

diagnose user device filter negate vd

Negate parameter.

```
diagnose user device filter negate vd
```

diagnose user device filter vd

Index of virtual domain.

```
diagnose user device filter vd <index>
```

Parameter	Description	Type	Size
<index>	Index of virtual domain.	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 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 1839](#)
- [diagnose user-device-store device fortifone on page 1839](#)
- [diagnose user-device-store device fortifone add on page 1839](#)
- [diagnose user-device-store device fortifone delete on page 1839](#)
- [diagnose user-device-store device fortifone list on page 1840](#)
- [diagnose user-device-store device memory on page 1840](#)
- [diagnose user-device-store device memory list on page 1840](#)
- [diagnose user-device-store device memory mac-host on page 1840](#)
- [diagnose user-device-store device memory mac-host add on page 1840](#)
- [diagnose user-device-store device memory mac-host filter on page 1840](#)
- [diagnose user-device-store device memory mac-host modify on page 1841](#)
- [diagnose user-device-store device memory mac-host query on page 1841](#)
- [diagnose user-device-store device memory mac-host subscribe on page 1841](#)

- [diagnose user-device-store device memory mac-host subscribe disable on page 1841](#)
- [diagnose user-device-store device memory mac-host subscribe enable on page 1841](#)
- [diagnose user-device-store device memory mac-host validate on page 1842](#)
- [diagnose user-device-store device memory ot-purdue-set on page 1842](#)
- [diagnose user-device-store device memory query on page 1842](#)
- [diagnose user-device-store device memory uid on page 1842](#)
- [diagnose user-device-store device memory uid add on page 1842](#)
- [diagnose user-device-store device memory uid delete on page 1842](#)
- [diagnose user-device-store device memory uid update on page 1843](#)
- [diagnose user-device-store device memory vulnerability-detected on page 1843](#)
- [diagnose user-device-store device memory vulnerability-query on page 1843](#)
- [diagnose user-device-store device memory vulnerability-update on page 1843](#)
- [diagnose user-device-store device-stats-query on page 1843](#)
- [diagnose user-device-store device-stats-query filters-and on page 1844](#)
- [diagnose user-device-store device-stats-query filters-or on page 1844](#)
- [diagnose user-device-store email-stats on page 1844](#)
- [diagnose user-device-store email-stats list on page 1844](#)
- [diagnose user-device-store email-stats query on page 1844](#)
- [diagnose user-device-store fsw-device-stats-query on page 1844](#)
- [diagnose user-device-store fsw-device-stats-query filters-and on page 1845](#)
- [diagnose user-device-store fsw-device-stats-query filters-or on page 1845](#)
- [diagnose user-device-store ftcl-device-stats-query on page 1845](#)
- [diagnose user-device-store ftcl-device-stats-query filters-and on page 1845](#)
- [diagnose user-device-store ftcl-device-stats-query filters-or on page 1845](#)
- [diagnose user-device-store iot-ot-vuln on page 1846](#)
- [diagnose user-device-store iot-ot-vuln list on page 1846](#)
- [diagnose user-device-store iot-ot-vuln query on page 1846](#)
- [diagnose user-device-store unified on page 1846](#)
- [diagnose user-device-store unified clear on page 1846](#)
- [diagnose user-device-store unified debug on page 1846](#)
- [diagnose user-device-store unified debug disable on page 1847](#)
- [diagnose user-device-store unified debug enable on page 1847](#)
- [diagnose user-device-store unified delete on page 1847](#)
- [diagnose user-device-store unified device-memory-query on page 1847](#)
- [diagnose user-device-store unified device-memory-query filters-and on page 1847](#)
- [diagnose user-device-store unified device-memory-query filters-or on page 1847](#)
- [diagnose user-device-store unified device-query on page 1848](#)
- [diagnose user-device-store unified device-query filters-and on page 1848](#)
- [diagnose user-device-store unified device-query filters-or on page 1848](#)
- [diagnose user-device-store unified dump on page 1848](#)
- [diagnose user-device-store unified list on page 1848](#)
- [diagnose user-device-store unified re-query on page 1848](#)
- [diagnose user-device-store unified stats on page 1849](#)

- [diagnose user-device-store unified user-memory-query on page 1849](#)
- [diagnose user-device-store unified user-memory-query filters-and on page 1849](#)
- [diagnose user-device-store unified user-memory-query filters-or on page 1849](#)
- [diagnose user-device-store unified user-query on page 1849](#)
- [diagnose user-device-store unified user-query filters-and on page 1849](#)
- [diagnose user-device-store unified user-query filters-or on page 1850](#)
- [diagnose user-device-store user on page 1850](#)
- [diagnose user-device-store user memory on page 1850](#)
- [diagnose user-device-store user memory list on page 1850](#)
- [diagnose user-device-store user memory query on page 1850](#)
- [diagnose user-device-store user-count on page 1850](#)
- [diagnose user-device-store user-count list on page 1851](#)
- [diagnose user-device-store user-count query on page 1851](#)
- [diagnose user-device-store user-stats on page 1851](#)
- [diagnose user-device-store user-stats query on page 1851](#)

diagnose user-device-store device

Device sessions info.

```
diagnose user-device-store device
```

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/Modify/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 filter

Query mac host info with filter by <vdom> <mac> <ip-from> [ip-to].

```
diagnose user-device-store device memory mac-host filter
```

diagnose user-device-store device memory mac-host modify

Modify by <vdom> <mac> <ip>.

```
diagnose user-device-store device memory mac-host modify
```

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-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 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 1851](#)
- [diagnose vendor-mac id-summary on page 1852](#)
- [diagnose vendor-mac info on page 1852](#)
- [diagnose vendor-mac match on page 1852](#)

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 vmware

VMWare platform diagnose commands.

This topic includes the following commands:

- [diagnose vmware ovfenv on page 1853](#)

diagnose vmware ovfenv

Display OVF environment information.

```
diagnose vmware ovfenv
```

diagnose vpn ssl

SSL-VPN.

```
diagnose vpn ssl
```

diagnose wacs

Web cache DB daemon.

This topic includes the following commands:

- [diagnose wacs clear on page 1853](#)
- [diagnose wacs restart on page 1853](#)
- [diagnose wacs stats on page 1854](#)

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 1867](#)
- [diagnose wad access-proxy health-check on page 1867](#)
- [diagnose wad access-proxy health-check status on page 1867](#)
- [diagnose wad config on page 1868](#)
- [diagnose wad config auth-rule on page 1868](#)
- [diagnose wad config policy on page 1868](#)
- [diagnose wad config proxy-policy on page 1868](#)
- [diagnose wad config summary on page 1868](#)
- [diagnose wad console-log on page 1868](#)
- [diagnose wad console-log disable on page 1869](#)
- [diagnose wad console-log enable on page 1869](#)
- [diagnose wad csvc on page 1869](#)
- [diagnose wad csvc bytercache on page 1869](#)
- [diagnose wad csvc bytercache clear on page 1869](#)
- [diagnose wad csvc bytercache flush on page 1869](#)
- [diagnose wad csvc bytercache lists on page 1870](#)
- [diagnose wad csvc bytercache stats on page 1870](#)
- [diagnose wad csvc bytercache toggle on page 1870](#)
- [diagnose wad csvc bytercache toggle all on page 1870](#)
- [diagnose wad csvc bytercache toggle create on page 1871](#)
- [diagnose wad csvc bytercache toggle read on page 1871](#)
- [diagnose wad csvc memcache on page 1871](#)
- [diagnose wad csvc memcache clear on page 1871](#)
- [diagnose wad csvc memcache flush on page 1871](#)
- [diagnose wad csvc memcache lists on page 1872](#)
- [diagnose wad csvc memcache stats on page 1872](#)
- [diagnose wad csvc restart on page 1872](#)
- [diagnose wad csvc webcache on page 1872](#)
- [diagnose wad csvc webcache clear on page 1873](#)
- [diagnose wad csvc webcache flush on page 1873](#)

- [diagnose wad csvc webcache lists on page 1873](#)
- [diagnose wad csvc webcache stats on page 1873](#)
- [diagnose wad csvc webcache toggle on page 1873](#)
- [diagnose wad csvc webcache toggle abort on page 1874](#)
- [diagnose wad csvc webcache toggle add_ref on page 1874](#)
- [diagnose wad csvc webcache toggle all on page 1874](#)
- [diagnose wad csvc webcache toggle append on page 1874](#)
- [diagnose wad csvc webcache toggle create on page 1875](#)
- [diagnose wad csvc webcache toggle read on page 1875](#)
- [diagnose wad csvc webcache toggle remove on page 1875](#)
- [diagnose wad csvc webcache toggle resolve on page 1875](#)
- [diagnose wad csvc webcache toggle update on page 1875](#)
- [diagnose wad debug on page 1876](#)
- [diagnose wad debug clear on page 1876](#)
- [diagnose wad debug crash on page 1876](#)
- [diagnose wad debug crash clear on page 1876](#)
- [diagnose wad debug crash disable on page 1876](#)
- [diagnose wad debug crash enable on page 1876](#)
- [diagnose wad debug crash list on page 1877](#)
- [diagnose wad debug crash max on page 1877](#)
- [diagnose wad debug crash read on page 1877](#)
- [diagnose wad debug disable on page 1877](#)
- [diagnose wad debug disable category on page 1877](#)
- [diagnose wad debug disable category aio on page 1878](#)
- [diagnose wad debug disable category antiphish on page 1878](#)
- [diagnose wad debug disable category auth on page 1878](#)
- [diagnose wad debug disable category autotest on page 1878](#)
- [diagnose wad debug disable category bytcache on page 1878](#)
- [diagnose wad debug disable category cache_server on page 1878](#)
- [diagnose wad debug disable category casb on page 1879](#)
- [diagnose wad debug disable category cifs on page 1879](#)
- [diagnose wad debug disable category cmgr on page 1879](#)
- [diagnose wad debug disable category config on page 1879](#)
- [diagnose wad debug disable category csvc on page 1879](#)
- [diagnose wad debug disable category detail on page 1879](#)
- [diagnose wad debug disable category devuln on page 1880](#)
- [diagnose wad debug disable category diag on page 1880](#)
- [diagnose wad debug disable category dispatcher on page 1880](#)
- [diagnose wad debug disable category dns on page 1880](#)
- [diagnose wad debug disable category dskd on page 1880](#)
- [diagnose wad debug disable category email on page 1880](#)
- [diagnose wad debug disable category extension on page 1881](#)
- [diagnose wad debug disable category ftp on page 1881](#)

- [diagnose wad debug disable category http on page 1881](#)
- [diagnose wad debug disable category http2 on page 1881](#)
- [diagnose wad debug disable category http3 on page 1881](#)
- [diagnose wad debug disable category icap on page 1881](#)
- [diagnose wad debug disable category icap_server on page 1882](#)
- [diagnose wad debug disable category icbsvc on page 1882](#)
- [diagnose wad debug disable category info on page 1882](#)
- [diagnose wad debug disable category ips on page 1882](#)
- [diagnose wad debug disable category isolator on page 1882](#)
- [diagnose wad debug disable category license on page 1882](#)
- [diagnose wad debug disable category mapi on page 1883](#)
- [diagnose wad debug disable category memblk on page 1883](#)
- [diagnose wad debug disable category monitor on page 1883](#)
- [diagnose wad debug disable category packet on page 1883](#)
- [diagnose wad debug disable category policy on page 1883](#)
- [diagnose wad debug disable category policy_test on page 1883](#)
- [diagnose wad debug disable category proc on page 1884](#)
- [diagnose wad debug disable category quic on page 1884](#)
- [diagnose wad debug disable category quic_cc on page 1884](#)
- [diagnose wad debug disable category rev_conn on page 1884](#)
- [diagnose wad debug disable category rpc on page 1884](#)
- [diagnose wad debug disable category scan on page 1884](#)
- [diagnose wad debug disable category scp on page 1885](#)
- [diagnose wad debug disable category session on page 1885](#)
- [diagnose wad debug disable category sftp on page 1885](#)
- [diagnose wad debug disable category socks on page 1885](#)
- [diagnose wad debug disable category ssh on page 1885](#)
- [diagnose wad debug disable category ssl on page 1885](#)
- [diagnose wad debug disable category stream on page 1886](#)
- [diagnose wad debug disable category svc_conn on page 1886](#)
- [diagnose wad debug disable category sys on page 1886](#)
- [diagnose wad debug disable category tls_fingerprint on page 1886](#)
- [diagnose wad debug disable category tunnel on page 1886](#)
- [diagnose wad debug disable category uih on page 1886](#)
- [diagnose wad debug disable category video on page 1887](#)
- [diagnose wad debug disable category vs on page 1887](#)
- [diagnose wad debug disable category waf on page 1887](#)
- [diagnose wad debug disable category webcache on page 1887](#)
- [diagnose wad debug disable category ztna_portal on page 1887](#)
- [diagnose wad debug display on page 1887](#)
- [diagnose wad debug display pid on page 1888](#)
- [diagnose wad debug display pid disable on page 1888](#)
- [diagnose wad debug display pid enable on page 1888](#)

- [diagnose wad debug enable on page 1888](#)
- [diagnose wad debug enable all on page 1888](#)
- [diagnose wad debug enable category on page 1888](#)
- [diagnose wad debug enable category aio on page 1889](#)
- [diagnose wad debug enable category all on page 1889](#)
- [diagnose wad debug enable category antiphish on page 1889](#)
- [diagnose wad debug enable category auth on page 1889](#)
- [diagnose wad debug enable category autotest on page 1889](#)
- [diagnose wad debug enable category bytcache on page 1889](#)
- [diagnose wad debug enable category cache_server on page 1890](#)
- [diagnose wad debug enable category casb on page 1890](#)
- [diagnose wad debug enable category cifs on page 1890](#)
- [diagnose wad debug enable category cmgr on page 1890](#)
- [diagnose wad debug enable category config on page 1890](#)
- [diagnose wad debug enable category csvc on page 1890](#)
- [diagnose wad debug enable category detail on page 1891](#)
- [diagnose wad debug enable category devuln on page 1891](#)
- [diagnose wad debug enable category diag on page 1891](#)
- [diagnose wad debug enable category dispatcher on page 1891](#)
- [diagnose wad debug enable category dns on page 1891](#)
- [diagnose wad debug enable category dskd on page 1891](#)
- [diagnose wad debug enable category email on page 1892](#)
- [diagnose wad debug enable category extension on page 1892](#)
- [diagnose wad debug enable category ftp on page 1892](#)
- [diagnose wad debug enable category http on page 1892](#)
- [diagnose wad debug enable category http2 on page 1892](#)
- [diagnose wad debug enable category http3 on page 1892](#)
- [diagnose wad debug enable category icap on page 1893](#)
- [diagnose wad debug enable category icap_server on page 1893](#)
- [diagnose wad debug enable category icbsvc on page 1893](#)
- [diagnose wad debug enable category info on page 1893](#)
- [diagnose wad debug enable category ips on page 1893](#)
- [diagnose wad debug enable category isolator on page 1893](#)
- [diagnose wad debug enable category license on page 1894](#)
- [diagnose wad debug enable category mapi on page 1894](#)
- [diagnose wad debug enable category memblk on page 1894](#)
- [diagnose wad debug enable category monitor on page 1894](#)
- [diagnose wad debug enable category packet on page 1894](#)
- [diagnose wad debug enable category policy on page 1894](#)
- [diagnose wad debug enable category policy_test on page 1895](#)
- [diagnose wad debug enable category proc on page 1895](#)
- [diagnose wad debug enable category quic on page 1895](#)
- [diagnose wad debug enable category quic_cc on page 1895](#)

- [diagnose wad debug enable category rev_conn on page 1895](#)
- [diagnose wad debug enable category rpc on page 1895](#)
- [diagnose wad debug enable category scan on page 1896](#)
- [diagnose wad debug enable category scp on page 1896](#)
- [diagnose wad debug enable category session on page 1896](#)
- [diagnose wad debug enable category sftp on page 1896](#)
- [diagnose wad debug enable category socks on page 1896](#)
- [diagnose wad debug enable category ssh on page 1896](#)
- [diagnose wad debug enable category ssl on page 1897](#)
- [diagnose wad debug enable category stream on page 1897](#)
- [diagnose wad debug enable category svc_conn on page 1897](#)
- [diagnose wad debug enable category sys on page 1897](#)
- [diagnose wad debug enable category tls_fingerprint on page 1897](#)
- [diagnose wad debug enable category tunnel on page 1897](#)
- [diagnose wad debug enable category uih on page 1898](#)
- [diagnose wad debug enable category video on page 1898](#)
- [diagnose wad debug enable category vs on page 1898](#)
- [diagnose wad debug enable category waf on page 1898](#)
- [diagnose wad debug enable category webcache on page 1898](#)
- [diagnose wad debug enable category ztna_portal on page 1898](#)
- [diagnose wad debug enable level on page 1899](#)
- [diagnose wad debug enable level error on page 1899](#)
- [diagnose wad debug enable level info on page 1899](#)
- [diagnose wad debug enable level verbose on page 1899](#)
- [diagnose wad debug enable level warn on page 1899](#)
- [diagnose wad debug ips-db on page 1900](#)
- [diagnose wad debug ips-db status on page 1900](#)
- [diagnose wad debug ips-filter on page 1900](#)
- [diagnose wad debug ips-filter aid on page 1900](#)
- [diagnose wad debug ips-filter all on page 1900](#)
- [diagnose wad debug ips-filter clear on page 1900](#)
- [diagnose wad debug ips-filter show on page 1901](#)
- [diagnose wad debug ips-filter vid on page 1901](#)
- [diagnose wad debug save-http-req-crash on page 1901](#)
- [diagnose wad debug save-http-req-crash disable on page 1901](#)
- [diagnose wad debug save-http-req-crash enable on page 1901](#)
- [diagnose wad debug show on page 1901](#)
- [diagnose wad dev on page 1902](#)
- [diagnose wad dev fcnacd on page 1902](#)
- [diagnose wad dev fcnacd delete on page 1902](#)
- [diagnose wad dev fcnacd ip-err on page 1902](#)
- [diagnose wad dev fcnacd uid-err on page 1902](#)
- [diagnose wad dev fcnacd update on page 1902](#)

- [diagnose wad dev query-by on page 1903](#)
- [diagnose wad dev query-by ipv4 on page 1903](#)
- [diagnose wad dev query-by ipv6 on page 1903](#)
- [diagnose wad dev query-by uid on page 1903](#)
- [diagnose wad dev-vuln on page 1903](#)
- [diagnose wad dev-vuln query on page 1903](#)
- [diagnose wad dev-vuln query-by-id on page 1904](#)
- [diagnose wad dev-vuln query-ftgd on page 1904](#)
- [diagnose wad dynamic-bypass on page 1904](#)
- [diagnose wad dynamic-bypass clear on page 1904](#)
- [diagnose wad dynamic-bypass flush on page 1904](#)
- [diagnose wad dynamic-bypass show on page 1904](#)
- [diagnose wad exp-fw-policy-test on page 1905](#)
- [diagnose wad exp-fw-policy-test-save on page 1905](#)
- [diagnose wad filter on page 1905](#)
- [diagnose wad filter clear on page 1906](#)
- [diagnose wad filter dport on page 1906](#)
- [diagnose wad filter drop-unknown-session on page 1906](#)
- [diagnose wad filter dst on page 1906](#)
- [diagnose wad filter dst6 on page 1906](#)
- [diagnose wad filter explicit-policy on page 1907](#)
- [diagnose wad filter firewall-policy on page 1907](#)
- [diagnose wad filter list on page 1907](#)
- [diagnose wad filter negate on page 1907](#)
- [diagnose wad filter process-id on page 1908](#)
- [diagnose wad filter process-id-by-src on page 1908](#)
- [diagnose wad filter process-type on page 1908](#)
- [diagnose wad filter protocol on page 1908](#)
- [diagnose wad filter proxy-policy-list-increment on page 1909](#)
- [diagnose wad filter sport on page 1909](#)
- [diagnose wad filter src on page 1909](#)
- [diagnose wad filter src6 on page 1910](#)
- [diagnose wad filter vd on page 1910](#)
- [diagnose wad fw-policy-test-get on page 1910](#)
- [diagnose wad health on page 1910](#)
- [diagnose wad health debug on page 1910](#)
- [diagnose wad health fs on page 1911](#)
- [diagnose wad health worker on page 1911](#)
- [diagnose wad history on page 1911](#)
- [diagnose wad history clear on page 1911](#)
- [diagnose wad history list on page 1911](#)
- [diagnose wad icap on page 1912](#)
- [diagnose wad icap list on page 1912](#)

- [diagnose wad kxp on page 1912](#)
- [diagnose wad kxp clear on page 1912](#)
- [diagnose wad kxp list on page 1912](#)
- [diagnose wad license on page 1912](#)
- [diagnose wad license clear on page 1913](#)
- [diagnose wad license debug on page 1913](#)
- [diagnose wad license debug fcas on page 1913](#)
- [diagnose wad license debug fnbi on page 1913](#)
- [diagnose wad license debug furl on page 1913](#)
- [diagnose wad license detail on page 1914](#)
- [diagnose wad license glob-usage on page 1914](#)
- [diagnose wad license glob-usage 15seconds on page 1914](#)
- [diagnose wad license glob-usage 5minutes on page 1914](#)
- [diagnose wad license glob-usage days on page 1914](#)
- [diagnose wad license glob-usage hours on page 1914](#)
- [diagnose wad license glob-usage months on page 1915](#)
- [diagnose wad license glob-usage weeks on page 1915](#)
- [diagnose wad license glob-usage years on page 1915](#)
- [diagnose wad license summary on page 1915](#)
- [diagnose wad license test on page 1915](#)
- [diagnose wad license usage on page 1915](#)
- [diagnose wad license usage 15seconds on page 1916](#)
- [diagnose wad license usage 5minutes on page 1916](#)
- [diagnose wad license usage days on page 1916](#)
- [diagnose wad license usage hours on page 1916](#)
- [diagnose wad license usage months on page 1916](#)
- [diagnose wad license usage weeks on page 1916](#)
- [diagnose wad license usage years on page 1917](#)
- [diagnose wad memory on page 1917](#)
- [diagnose wad memory monitor on page 1917](#)
- [diagnose wad memory monitor disable on page 1917](#)
- [diagnose wad memory monitor enable on page 1917](#)
- [diagnose wad memory monitor interval on page 1917](#)
- [diagnose wad memory monitor list on page 1918](#)
- [diagnose wad memory monitor max-report-files on page 1918](#)
- [diagnose wad memory monitor mem-threshold-red on page 1918](#)
- [diagnose wad memory overused on page 1918](#)
- [diagnose wad memory report on page 1918](#)
- [diagnose wad memory sum on page 1919](#)
- [diagnose wad memory track on page 1919](#)
- [diagnose wad memory workers on page 1919](#)
- [diagnose wad nbi on page 1919](#)
- [diagnose wad nbi license on page 1919](#)

- [diagnose wad nbi packages on page 1920](#)
- [diagnose wad nbi status on page 1920](#)
- [diagnose wad process on page 1920](#)
- [diagnose wad process YouTube-filter-cache-service on page 1920](#)
- [diagnose wad process algo on page 1920](#)
- [diagnose wad process byte-cache on page 1921](#)
- [diagnose wad process cache-service-cs on page 1921](#)
- [diagnose wad process cache-service-db on page 1921](#)
- [diagnose wad process cert-inspection on page 1922](#)
- [diagnose wad process cert-manager on page 1922](#)
- [diagnose wad process config-notify on page 1922](#)
- [diagnose wad process debug on page 1923](#)
- [diagnose wad process dev-vuln on page 1923](#)
- [diagnose wad process dispatcher on page 1923](#)
- [diagnose wad process ia-cache on page 1924](#)
- [diagnose wad process informer on page 1924](#)
- [diagnose wad process isolator on page 1924](#)
- [diagnose wad process manager on page 1925](#)
- [diagnose wad process object-cache on page 1925](#)
- [diagnose wad process preload daemon on page 1925](#)
- [diagnose wad process reverse-connector on page 1926](#)
- [diagnose wad process staled-worker on page 1926](#)
- [diagnose wad process tls-fgpt-service on page 1926](#)
- [diagnose wad process traffic aggregator on page 1927](#)
- [diagnose wad process unknown on page 1927](#)
- [diagnose wad process user-info on page 1927](#)
- [diagnose wad process user-info-history on page 1928](#)
- [diagnose wad process worker on page 1928](#)
- [diagnose wad report on page 1928](#)
- [diagnose wad report policy on page 1928](#)
- [diagnose wad report session on page 1929](#)
- [diagnose wad report user on page 1929](#)
- [diagnose wad restore on page 1929](#)
- [diagnose wad restore cdn-rules on page 1929](#)
- [diagnose wad restore cdn-rules all on page 1929](#)
- [diagnose wad session on page 1929](#)
- [diagnose wad session clear on page 1930](#)
- [diagnose wad session list on page 1930](#)
- [diagnose wad session list-http2 on page 1930](#)
- [diagnose wad sshproxy on page 1930](#)
- [diagnose wad sshproxy clear on page 1930](#)
- [diagnose wad sshproxy list on page 1930](#)
- [diagnose wad stats on page 1931](#)

- [diagnose wad stats algo on page 1931](#)
- [diagnose wad stats algo.antiphish on page 1931](#)
- [diagnose wad stats algo.casb on page 1931](#)
- [diagnose wad stats algo.dev_info on page 1932](#)
- [diagnose wad stats algo.dev_type on page 1932](#)
- [diagnose wad stats algo.fast_tb on page 1932](#)
- [diagnose wad stats algo.fw_policy on page 1932](#)
- [diagnose wad stats algo.icap_client on page 1932](#)
- [diagnose wad stats algo.ips on page 1933](#)
- [diagnose wad stats algo.ips_builder on page 1933](#)
- [diagnose wad stats algo.krl on page 1933](#)
- [diagnose wad stats algo.proc_common on page 1933](#)
- [diagnose wad stats algo.sec_prof on page 1934](#)
- [diagnose wad stats algo.ssl on page 1934](#)
- [diagnose wad stats algo.url_filter on page 1934](#)
- [diagnose wad stats algo.urlredirect on page 1934](#)
- [diagnose wad stats cache_service on page 1935](#)
- [diagnose wad stats cache_service.proc_common on page 1935](#)
- [diagnose wad stats cache_service.tcp on page 1935](#)
- [diagnose wad stats cic on page 1935](#)
- [diagnose wad stats cic.proc_common on page 1935](#)
- [diagnose wad stats cmgr on page 1936](#)
- [diagnose wad stats cmgr.cert_cache on page 1936](#)
- [diagnose wad stats cmgr.cert_service on page 1936](#)
- [diagnose wad stats cmgr.dns_req on page 1936](#)
- [diagnose wad stats cmgr.http_engine on page 1937](#)
- [diagnose wad stats cmgr.proc_common on page 1937](#)
- [diagnose wad stats cmgr.quic on page 1937](#)
- [diagnose wad stats cmgr.ssl on page 1937](#)
- [diagnose wad stats cmgr.tcp on page 1938](#)
- [diagnose wad stats common on page 1938](#)
- [diagnose wad stats common.dc_ad_dns on page 1938](#)
- [diagnose wad stats common.diag on page 1938](#)
- [diagnose wad stats common.sched on page 1938](#)
- [diagnose wad stats common.ses_stats on page 1939](#)
- [diagnose wad stats common.waps on page 1939](#)
- [diagnose wad stats config on page 1939](#)
- [diagnose wad stats config.proc_common on page 1939](#)
- [diagnose wad stats config.shm_stats on page 1940](#)
- [diagnose wad stats config.stream_scan on page 1940](#)
- [diagnose wad stats debug on page 1940](#)
- [diagnose wad stats debug.crash_handler on page 1940](#)
- [diagnose wad stats debug.proc_common on page 1941](#)

- [diagnose wad stats dev_vuln on page 1941](#)
- [diagnose wad stats dev_vuln.dns_req on page 1941](#)
- [diagnose wad stats dev_vuln.proc_common on page 1941](#)
- [diagnose wad stats dev_vuln.ssl on page 1941](#)
- [diagnose wad stats dev_vuln.tcp on page 1942](#)
- [diagnose wad stats dispatcher on page 1942](#)
- [diagnose wad stats dispatcher.cifs on page 1942](#)
- [diagnose wad stats dispatcher.dns_proxy on page 1942](#)
- [diagnose wad stats dispatcher.icap_local_server on page 1943](#)
- [diagnose wad stats dispatcher.proc_common on page 1943](#)
- [diagnose wad stats dispatcher.ssh on page 1943](#)
- [diagnose wad stats dispatcher.tcp on page 1943](#)
- [diagnose wad stats dispatcher.tunnel on page 1944](#)
- [diagnose wad stats fgpt on page 1944](#)
- [diagnose wad stats fgpt.proc_common on page 1944](#)
- [diagnose wad stats ia_cache on page 1944](#)
- [diagnose wad stats ia_cache.proc_common on page 1944](#)
- [diagnose wad stats informer on page 1945](#)
- [diagnose wad stats informer.dev_info on page 1945](#)
- [diagnose wad stats informer.dev_type on page 1945](#)
- [diagnose wad stats informer.proc_common on page 1945](#)
- [diagnose wad stats informer.ztna_jwt on page 1946](#)
- [diagnose wad stats isolator on page 1946](#)
- [diagnose wad stats isolator.dns_req on page 1946](#)
- [diagnose wad stats isolator.proc_common on page 1946](#)
- [diagnose wad stats isolator.ssl on page 1947](#)
- [diagnose wad stats isolator.tcp on page 1947](#)
- [diagnose wad stats mgr on page 1947](#)
- [diagnose wad stats mgr.proc_common on page 1947](#)
- [diagnose wad stats mgr.shm_stats on page 1947](#)
- [diagnose wad stats uih on page 1948](#)
- [diagnose wad stats uih.proc_common on page 1948](#)
- [diagnose wad stats usr_info on page 1948](#)
- [diagnose wad stats usr_info.dev_info on page 1948](#)
- [diagnose wad stats usr_info.dev_type on page 1949](#)
- [diagnose wad stats usr_info.dns_req on page 1949](#)
- [diagnose wad stats usr_info.proc_common on page 1949](#)
- [diagnose wad stats usr_info.ssl on page 1949](#)
- [diagnose wad stats usr_info.tcp on page 1950](#)
- [diagnose wad stats vfcs on page 1950](#)
- [diagnose wad stats vfcs.proc_common on page 1950](#)
- [diagnose wad stats worker on page 1950](#)
- [diagnose wad stats worker.aio on page 1950](#)

- [diagnose wad stats worker.antiphish on page 1951](#)
- [diagnose wad stats worker.app_mgr on page 1951](#)
- [diagnose wad stats worker.auth on page 1951](#)
- [diagnose wad stats worker.casb on page 1951](#)
- [diagnose wad stats worker.cert_cache on page 1952](#)
- [diagnose wad stats worker.cifs on page 1952](#)
- [diagnose wad stats worker.config_delta on page 1952](#)
- [diagnose wad stats worker.conn_pool on page 1952](#)
- [diagnose wad stats worker.dev_info on page 1953](#)
- [diagnose wad stats worker.dev_type on page 1953](#)
- [diagnose wad stats worker.dns_proxy on page 1953](#)
- [diagnose wad stats worker.dns_req on page 1953](#)
- [diagnose wad stats worker.fast_match on page 1953](#)
- [diagnose wad stats worker.fw_policy on page 1954](#)
- [diagnose wad stats worker.hauth_uid_cache on page 1954](#)
- [diagnose wad stats worker.http_engine on page 1954](#)
- [diagnose wad stats worker.http_ffbk on page 1954](#)
- [diagnose wad stats worker.http_scan on page 1955](#)
- [diagnose wad stats worker.http_srv_selector on page 1955](#)
- [diagnose wad stats worker.http_view on page 1955](#)
- [diagnose wad stats worker.icap_client on page 1955](#)
- [diagnose wad stats worker.icap_local_server on page 1956](#)
- [diagnose wad stats worker.icap_parser on page 1956](#)
- [diagnose wad stats worker.icap_remote_server on page 1956](#)
- [diagnose wad stats worker.infection_cache on page 1956](#)
- [diagnose wad stats worker.ipseng on page 1956](#)
- [diagnose wad stats worker.krl on page 1957](#)
- [diagnose wad stats worker.pol_test on page 1957](#)
- [diagnose wad stats worker.policy_profile on page 1957](#)
- [diagnose wad stats worker.proc_common on page 1957](#)
- [diagnose wad stats worker.protos on page 1958](#)
- [diagnose wad stats worker.quic on page 1958](#)
- [diagnose wad stats worker.scan_cache on page 1958](#)
- [diagnose wad stats worker.sec_prof on page 1958](#)
- [diagnose wad stats worker.shm_stats on page 1959](#)
- [diagnose wad stats worker.ssh on page 1959](#)
- [diagnose wad stats worker.ssl on page 1959](#)
- [diagnose wad stats worker.sysmem on page 1959](#)
- [diagnose wad stats worker.tcp on page 1959](#)
- [diagnose wad stats worker.traffic_mirror on page 1960](#)
- [diagnose wad stats worker.tunnel on page 1960](#)
- [diagnose wad stats worker.url_filter on page 1960](#)
- [diagnose wad stats worker.url_match on page 1960](#)

- [diagnose wad stats worker.urlredirect on page 1961](#)
- [diagnose wad stats worker.vs_cert_cache on page 1961](#)
- [diagnose wad stats worker.ztna_jwt on page 1961](#)
- [diagnose wad stream-scan on page 1961](#)
- [diagnose wad stream-scan av-intf on page 1962](#)
- [diagnose wad stream-scan av-intf disable on page 1962](#)
- [diagnose wad stream-scan av-intf enable on page 1962](#)
- [diagnose wad stream-scan av-test on page 1962](#)
- [diagnose wad tcp-connection on page 1962](#)
- [diagnose wad tcp-connection list on page 1962](#)
- [diagnose wad toggle on page 1963](#)
- [diagnose wad tp-fw-policy-test on page 1963](#)
- [diagnose wad tp-fw-policy-test-save on page 1963](#)
- [diagnose wad tunnel on page 1964](#)
- [diagnose wad tunnel clear on page 1964](#)
- [diagnose wad tunnel list on page 1964](#)
- [diagnose wad uih on page 1964](#)
- [diagnose wad uih chart on page 1965](#)
- [diagnose wad uih chart range on page 1965](#)
- [diagnose wad uih chart summary on page 1965](#)
- [diagnose wad url-lookup on page 1965](#)
- [diagnose wad user on page 1965](#)
- [diagnose wad user clear on page 1965](#)
- [diagnose wad user count on page 1966](#)
- [diagnose wad user device on page 1966](#)
- [diagnose wad user domain-controller on page 1966](#)
- [diagnose wad user domain-controller dns on page 1966](#)
- [diagnose wad user domain-controller dns list on page 1966](#)
- [diagnose wad user domain-controller dns test on page 1967](#)
- [diagnose wad user exchange on page 1967](#)
- [diagnose wad user exchange get-matches on page 1967](#)
- [diagnose wad user exchange query-rows on page 1967](#)
- [diagnose wad user exchange reset on page 1967](#)
- [diagnose wad user exchange resolve-names on page 1967](#)
- [diagnose wad user exchange test-auto-discover on page 1968](#)
- [diagnose wad user list on page 1968](#)
- [diagnose wad webcache on page 1968](#)
- [diagnose wad webcache clear on page 1968](#)
- [diagnose wad webcache list on page 1968](#)
- [diagnose wad webproxy on page 1969](#)
- [diagnose wad webproxy clear on page 1969](#)
- [diagnose wad webproxy forward-server on page 1969](#)
- [diagnose wad webproxy forward-server detail on page 1969](#)

- [diagnose wad webproxy forward-server summary on page 1969](#)
- [diagnose wad webproxy forward-server-group on page 1969](#)
- [diagnose wad webproxy list on page 1970](#)
- [diagnose wad worker on page 1970](#)
- [diagnose wad worker async-ut on page 1970](#)
- [diagnose wad worker avscan on page 1970](#)
- [diagnose wad worker avscan clear on page 1970](#)
- [diagnose wad worker avscan list on page 1970](#)
- [diagnose wad worker bytcache on page 1971](#)
- [diagnose wad worker bytcache clear on page 1971](#)
- [diagnose wad worker bytcache flush on page 1971](#)
- [diagnose wad worker bytcache stats on page 1971](#)
- [diagnose wad worker bytcache toggle on page 1971](#)
- [diagnose wad worker bytcache toggle all on page 1972](#)
- [diagnose wad worker bytcache toggle config on page 1972](#)
- [diagnose wad worker bytcache toggle create on page 1972](#)
- [diagnose wad worker bytcache toggle read on page 1972](#)
- [diagnose wad worker cookie on page 1972](#)
- [diagnose wad worker cookie map on page 1973](#)
- [diagnose wad worker filter on page 1973](#)
- [diagnose wad worker filter clear on page 1973](#)
- [diagnose wad worker filter list on page 1973](#)
- [diagnose wad worker imagecache on page 1973](#)
- [diagnose wad worker imagecache flush on page 1973](#)
- [diagnose wad worker imagecache stats on page 1974](#)
- [diagnose wad worker memcache on page 1974](#)
- [diagnose wad worker memcache clear on page 1974](#)
- [diagnose wad worker memcache flush on page 1974](#)
- [diagnose wad worker memcache stats on page 1974](#)
- [diagnose wad worker memcache toggle on page 1975](#)
- [diagnose wad worker memcache toggle all on page 1975](#)
- [diagnose wad worker memcache toggle config on page 1975](#)
- [diagnose wad worker memcache toggle create on page 1975](#)
- [diagnose wad worker memcache toggle read on page 1975](#)
- [diagnose wad worker oidc on page 1976](#)
- [diagnose wad worker oidc clear-jwks on page 1976](#)
- [diagnose wad worker oidc refresh-server on page 1976](#)
- [diagnose wad worker oidc servers on page 1976](#)
- [diagnose wad worker oidc sessions on page 1977](#)
- [diagnose wad worker peer on page 1977](#)
- [diagnose wad worker peer clear on page 1977](#)
- [diagnose wad worker peer list on page 1977](#)
- [diagnose wad worker policy on page 1977](#)

- [diagnose wad worker policy clear on page 1977](#)
- [diagnose wad worker policy list on page 1978](#)
- [diagnose wad worker restart on page 1978](#)
- [diagnose wad worker saml on page 1978](#)
- [diagnose wad worker scripts on page 1978](#)
- [diagnose wad worker scripts clear on page 1978](#)
- [diagnose wad worker scripts list on page 1979](#)
- [diagnose wad worker webcache on page 1979](#)
- [diagnose wad worker webcache clear on page 1979](#)
- [diagnose wad worker webcache flush on page 1979](#)
- [diagnose wad worker webcache stats on page 1979](#)
- [diagnose wad worker webcache summary on page 1980](#)
- [diagnose wad worker webcache toggle on page 1980](#)
- [diagnose wad worker webcache toggle abort on page 1980](#)
- [diagnose wad worker webcache toggle add_ref on page 1980](#)
- [diagnose wad worker webcache toggle all on page 1980](#)
- [diagnose wad worker webcache toggle append on page 1981](#)
- [diagnose wad worker webcache toggle config on page 1981](#)
- [diagnose wad worker webcache toggle create on page 1981](#)
- [diagnose wad worker webcache toggle read on page 1981](#)
- [diagnose wad worker webcache toggle remove on page 1981](#)
- [diagnose wad worker webcache toggle resolve on page 1982](#)
- [diagnose wad worker webcache toggle update on page 1982](#)

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>]	CSV C 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 aio

async io

```
diagnose wad debug disable category aio
```

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 cache_server

reverse cache server

```
diagnose wad debug disable category cache_server
```

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 extension

implicit proxy extension

```
diagnose wad debug disable category extension
```

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 icap_server

Local ICAP server

```
diagnose wad debug disable category icap_server
```

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 isolator

isolator

```
diagnose wad debug disable category isolator
```

diagnose wad debug disable category license

license

```
diagnose wad debug disable category license
```

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 rev_conn

ztna reverse connector

```
diagnose wad debug disable category rev_conn
```

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 tls_fingerprint

tls fintgerprint

```
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 waf

waf

```
diagnose wad debug disable category waf
```

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 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
```



This command may cause high CPU and memory usage due to large log volume.
To close, run `diag wad debug clear`.

diagnose wad debug enable category

Category debug setting.

```
diagnose wad debug enable category
```

diagnose wad debug enable category aio

async io

```
diagnose wad debug enable category aio
```

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 cache_server

reverse cache server

```
diagnose wad debug enable category cache_server
```

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 extension

implicit proxy extension

```
diagnose wad debug enable category extension
```

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 icap_server

Local ICAP server

```
diagnose wad debug enable category icap_server
```

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 isolator

isolator

```
diagnose wad debug enable category isolator
```

diagnose wad debug enable category license

license

```
diagnose wad debug enable category license
```

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 rev_conn

ztna reverse connector

```
diagnose wad debug enable category rev_conn
```

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 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 waf

waf

```
diagnose wad debug enable category waf
```

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 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
```



This command may cause high CPU and memory usage due to large log volume.
To close, run `diag wad debug clear`.

diagnose wad debug enable level verbose

verbose

```
diagnose wad debug enable level verbose
```



This command may cause high CPU and memory usage due to large log volume.
To close, run `diag wad debug clear`.

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 dynamic-bypass

Dynamic-bypass diagnostics.

```
diagnose wad dynamic-bypass
```

diagnose wad dynamic-bypass clear

Clear dynamic-bypass stats.

```
diagnose wad dynamic-bypass clear
```

diagnose wad dynamic-bypass flush

Flush dynamic-bypass entries.

```
diagnose wad dynamic-bypass flush
```

diagnose wad dynamic-bypass show

Show dynamic-bypass summary.

```
diagnose wad dynamic-bypass show
```

diagnose wad exp-fw-policy-test

Explicit firewall policy test.

```
diagnose wad exp-fw-policy-test <SRC> <WEBPROXY> <REQ> <AUTH_TYPE> <USER/GROUP> <SERVER>
```

Parameter	Description	Type	Size
<SRC>	Please input source IP.	string	
<WEBPROXY>	Please input webproxy name.	string	
<REQ>	Please input uri=<uri> or ipport=<ip:port> or multi-line http request.	string	
<AUTH_TYPE>	Please input authentication type: none, user or group.	string	
<USER/GROUP>	Please input username or name of matching user/group on remote authentication server.	string	
<SERVER>	Please input name of auth server.	string	

diagnose wad exp-fw-policy-test-save

Save explicit firewall policy test.

```
diagnose wad exp-fw-policy-test-save <SRC> <WEBPROXY> <REQ> <AUTH_TYPE> <USER/GROUP> <SERVER>
```

Parameter	Description	Type	Size
<SRC>	Please input source IP.	string	
<WEBPROXY>	Please input webproxy name.	string	
<REQ>	Please input uri=<uri> or ipport=<ip:port> or multi-line http request.	string	
<AUTH_TYPE>	Please input authentication type: none, user or group.	string	
<USER/GROUP>	Please input username or name of matching user/group on remote authentication server.	string	
<SERVER>	Please input name of auth server.	string	

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>
```

Parameter	Description	Type	Size
<port>	Destination port (from).	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>
```

Parameter	Description	Type	Size
<ip-address>	Destination IP address (from).	string	

diagnose wad filter dst6

Destination address6 range to filter by.

```
diagnose wad filter dst6 <ip-address6>
```

Parameter	Description	Type	Size
<ip-address6>	Destination IPv6 address (from).	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	
<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>
```

Parameter	Description	Type	Size
<port>	Source port (from).	string	

diagnose wad filter src

Source address range to filter by.

```
diagnose wad filter src <ip-address>
```

Parameter	Description	Type	Size
<ip-address>	Source IP address (from).	string	

diagnose wad filter src6

Source address6 range to filter by.

```
diagnose wad filter src6 <ip-address6>
```

Parameter	Description	Type	Size
<ip-address6>	Source IPv6 address (from).	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 fw-policy-test-get

Get firewall policy test.

```
diagnose wad fw-policy-test-get
```

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 diagnose 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 dianose 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 icap

ICAP diagnostics.

```
diagnose wad icap
```

diagnose wad icap list

List ICAP servers

```
diagnose wad icap list
```

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 license

Show License Info.

```
diagnose wad license
```

diagnose wad license clear

Clear all license usage history

```
diagnose wad license clear
```

diagnose wad license debug

Override license number for debug

```
diagnose wad license debug
```

diagnose wad license debug fcas

Set overriding licensed session limit for specified type

```
diagnose wad license debug fcas <limit>
```

Parameter	Description	Type	Size
<limit>	overriding licensed session limit (-1 to unset)	string	

diagnose wad license debug fnbi

Set overriding licensed session limit for specified type

```
diagnose wad license debug fnbi <limit>
```

Parameter	Description	Type	Size
<limit>	overriding licensed session limit (-1 to unset)	string	

diagnose wad license debug furl

Set overriding licensed session limit for specified type

```
diagnose wad license debug furl <limit>
```

Parameter	Description	Type	Size
<limit>	overriding licensed session limit (-1 to unset)	string	

diagnose wad license detail

Show License Detail.

```
diagnose wad license detail
```

diagnose wad license glob-usage

Show Total License Usage History of the Fabric Group

```
diagnose wad license glob-usage
```

diagnose wad license glob-usage 15seconds

15seconds

```
diagnose wad license glob-usage 15seconds
```

diagnose wad license glob-usage 5minutes

5minutes

```
diagnose wad license glob-usage 5minutes
```

diagnose wad license glob-usage days

days

```
diagnose wad license glob-usage days
```

diagnose wad license glob-usage hours

hours

```
diagnose wad license glob-usage hours
```

diagnose wad license glob-usage months

months

```
diagnose wad license glob-usage months
```

diagnose wad license glob-usage weeks

weeks

```
diagnose wad license glob-usage weeks
```

diagnose wad license glob-usage years

years

```
diagnose wad license glob-usage years
```

diagnose wad license summary

Show License summary.

```
diagnose wad license summary
```

diagnose wad license test

Add targeted value to test update function

```
diagnose wad license test <value> <repeats>
```

Parameter	Description	Type	Size
<value>	any non-negative integer in 0~65536	string	
<repeats>	any non-negative interger smaller than 2147483647	string	

diagnose wad license usage

Show License Usage History

```
diagnose wad license usage
```

diagnose wad license usage 15seconds

15seconds

```
diagnose wad license usage 15seconds
```

diagnose wad license usage 5minutes

5minutes

```
diagnose wad license usage 5minutes
```

diagnose wad license usage days

days

```
diagnose wad license usage days
```

diagnose wad license usage hours

hours

```
diagnose wad license usage hours
```

diagnose wad license usage months

months

```
diagnose wad license usage months
```

diagnose wad license usage weeks

weeks

```
diagnose wad license usage weeks
```


diagnose wad license usage years

years

```
diagnose wad license usage years
```

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
```



This command can spike CPU usage or block the CLI for seconds.

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>
```



This command can spike CPU usage or block the CLI for seconds.

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 nbi

Native Browser Isolator diagnostics.

```
diagnose wad nbi
```

diagnose wad nbi license

Show license information.

```
diagnose wad nbi license
```

diagnose wad nbi packages

List information for NBI packages.

```
diagnose wad nbi packages
```

diagnose wad nbi status

(Default) Display the full NBI status.

```
diagnose wad nbi status
```

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>
```

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	

diagnose wad process algo

Diagnose algo process.

```
diagnose wad process algo <index> <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	

diagnose wad process byte-cache

Diagnose byte-cache process.

```
diagnose wad process byte-cache <index> <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	

diagnose wad process cache-service-cs

Diagnose cache-service-cs process.

```
diagnose wad process cache-service-cs <index> <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	

diagnose wad process cache-service-db

Diagnose cache-service-db process.

```
diagnose wad process cache-service-db <index> <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	

diagnose wad process cert-inspection

Diagnose cert-inspection process.

```
diagnose wad process cert-inspection <index> <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	

diagnose wad process cert-manager

Diagnose cert-manager process.

```
diagnose wad process cert-manager <index> <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	

diagnose wad process config-notify

Diagnose config-notify process.

```
diagnose wad process config-notify <index> <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	

diagnose wad process debug

Diagnose debug process.

```
diagnose wad process debug <index> <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	

diagnose wad process dev-vuln

Diagnose dev-vuln process.

```
diagnose wad process dev-vuln <index> <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	

diagnose wad process dispatcher

Diagnose dispatcher process.

```
diagnose wad process dispatcher <index> <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	

diagnose wad process ia-cache

Diagnose ia-cache process.

```
diagnose wad process ia-cache <index> <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	

diagnose wad process informer

Diagnose informer process.

```
diagnose wad process informer <index> <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	

diagnose wad process isolator

Diagnose isolator process.

```
diagnose wad process isolator <index> <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	

diagnose wad process manager

Diagnose manager process.

```
diagnose wad process manager <index> <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	

diagnose wad process object-cache

Diagnose object-cache process.

```
diagnose wad process object-cache <index> <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	

diagnose wad process preload daemon

Diagnose preload daemon process.

```
diagnose wad process preload daemon <index> <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	

diagnose wad process reverse-connector

Diagnose reverse-connector process.

```
diagnose wad process reverse-connector <index> <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	

diagnose wad process staled-worker

Diagnose staled-worker process.

```
diagnose wad process staled-worker <index> <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	

diagnose wad process tls-fgpt-service

Diagnose tls-fgpt-service process.

```
diagnose wad process tls-fgpt-service <index> <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	

diagnose wad process traffic aggregator

Diagnose traffic aggregator process.

```
diagnose wad process traffic aggregator <index> <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	

diagnose wad process unknown

Diagnose unknown process.

```
diagnose wad process unknown <index> <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	

diagnose wad process user-info

Diagnose user-info process.

```
diagnose wad process user-info <index> <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	

diagnose wad process user-info-history

Diagnose user-info-history process.

```
diagnose wad process user-info-history <index> <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	

diagnose wad process worker

Diagnose worker process.

```
diagnose wad process worker <index> <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	

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 sshproxy

sshproxy diagnostics.

```
diagnose wad sshproxy
```

diagnose wad sshproxy clear

Clear sshproxy stats.

```
diagnose wad sshproxy clear
```

diagnose wad sshproxy list

List sshproxy stats.

```
diagnose wad sshproxy list
```

diagnose wad stats

Statistics.

```
diagnose wad stats <action>
```



This command can spike CPU usage or block the CLI for seconds.

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.fast_tb

Show fast_tb statistics.

```
diagnose wad stats algo.fast_tb <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.krl

Show krl statistics.

```
diagnose wad stats algo.krl <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 algo.urlredir

Show urlredir statistics.

```
diagnose wad stats algo.urlredir <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.shm_stats

Show shm_stats statistics.

```
diagnose wad stats config.shm_stats <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.icap_local_server

Show icap_local_server statistics.

```
diagnose wad stats dispatcher.icap_local_server <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 fgpt

Show proc_fgpt statistics.

```
diagnose wad stats fgpt <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats fgpt.proc_common

Show proc_common statistics.

```
diagnose wad stats fgpt.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats ia_cache

Show proc_ia_cache statistics.

```
diagnose wad stats ia_cache <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats ia_cache.proc_common

Show proc_common statistics.

```
diagnose wad stats ia_cache.proc_common <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.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 isolator

Show proc_isolator statistics.

```
diagnose wad stats isolator <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats isolator.dns_req

Show dns_req statistics.

```
diagnose wad stats isolator.dns_req <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats isolator.proc_common

Show proc_common statistics.

```
diagnose wad stats isolator.proc_common <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats isolator.ssl

Show ssl statistics.

```
diagnose wad stats isolator.ssl <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats isolator.tcp

Show tcp statistics.

```
diagnose wad stats isolator.tcp <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 mgr.shm_stats

Show shm_stats statistics.

```
diagnose wad stats mgr.shm_stats <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 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.aio

Show aio statistics.

```
diagnose wad stats worker.aio <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.auth

Show auth statistics.

```
diagnose wad stats worker.auth <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.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.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.http_view

Show http_view statistics.

```
diagnose wad stats worker.http_view <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_local_server

Show icap_local_server statistics.

```
diagnose wad stats worker.icap_local_server <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.krl

Show krl statistics.

```
diagnose wad stats worker.krl <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.scan_cache

Show scan_cache statistics.

```
diagnose wad stats worker.scan_cache <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.shm_stats

Show shm_stats statistics.

```
diagnose wad stats worker.shm_stats <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.url_match

Show url_match statistics.

```
diagnose wad stats worker.url_match <action>
```

Parameter	Description	Type	Size
<action>	show(default) clear history.	string	

diagnose wad stats worker.urlredir

Show urlredir statistics.

```
diagnose wad stats worker.urlredir <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 tcp-connection

TCP connection diagnostics.

```
diagnose wad tcp-connection
```

diagnose wad tcp-connection list

List first 100 tcp connections of each worker.

```
diagnose wad tcp-connection list <worker-index>/all
```

Parameter	Description	Type	Size
<worker-index>/all	Please enter worker index or all for all workers	string	

diagnose wad toggle

Toggle diagnose method(direct/debug proc).

```
diagnose wad toggle
```

diagnose wad tp-fw-policy-test

Transparent firewall policy test.

```
diagnose wad tp-fw-policy-test <SRC> <SRC-INTF> <REQ> <AUTH_TYPE> <USER/GROUP> <SERVER>
```

Parameter	Description	Type	Size
<SRC>	Please input source IP.	string	
<SRC-INTF>	Please input source interface.	string	
<REQ>	Please input uri=<uri> or ipport=<ip:port> or multi-line http request.	string	
<AUTH_TYPE>	Please input authentication type: none, user or group.	string	
<USER/GROUP>	Please input username or name of matching user/group on remote authentication server.	string	
<SERVER>	Please input name of auth server.	string	

diagnose wad tp-fw-policy-test-save

Save transparent firewall policy test.

```
diagnose wad tp-fw-policy-test-save <SRC> <SRC-INTF> <REQ> <AUTH_TYPE> <USER/GROUP> <SERVER>
```

Parameter	Description	Type	Size
<SRC>	Please input source IP.	string	

Parameter	Description	Type	Size
<SRC-INTF>	Please input source interface.	string	
<REQ>	Please input uri=<uri> or ipport=<ip:port> or multi-line http request.	string	
<AUTH_TYPE>	Please input authentication type: none, user or group.	string	
<USER/GROUP>	Please input username or name of matching user/group on remote authentication server.	string	
<SERVER>	Please input name of auth server.	string	

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 url-lookup

URL category/list lookup.

```
diagnose wad url-lookup <URL>
```

Parameter	Description	Type	Size
<URL>	Please input URL.	string	

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	
<IP>	Please input user IP.	string	
<VDOM>	Please input VDOM name the user belongs to.	string	

diagnose wad user count

Count users in each WAD worker.

```
diagnose wad user count
```

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 webproxy

Webproxy diagnostics.

```
diagnose wad webproxy
```

diagnose wad webproxy clear

Enter a webproxy name to clear this particular webproxy, otherwise this clears all webproxies.

```
diagnose wad webproxy clear <webproxy>
```

Parameter	Description	Type	Size
<webproxy>	webproxy name.	string	

diagnose wad webproxy forward-server

Forward server diagnostics.

```
diagnose wad webproxy forward-server
```

diagnose wad webproxy forward-server detail

Per worker forward server diagnostics.

```
diagnose wad webproxy forward-server detail
```

diagnose wad webproxy forward-server summary

General forward server diagnostics.

```
diagnose wad webproxy forward-server summary
```

diagnose wad webproxy forward-server-group

Forward server group diagnostics.

```
diagnose wad webproxy forward-server-group
```

diagnose wad webproxy list

List webproxies.

```
diagnose wad webproxy list
```

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

Bytcache 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 bytcache stats

Show statistics.

```
diagnose wad worker bytcache stats [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytcache toggle

Toggle operations.

```
diagnose wad worker bytcache 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 bytecache toggle create

Toggle create as busy.

```
diagnose wad worker bytecache toggle create [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker bytecache toggle read

Toggle read as busy.

```
diagnose wad worker bytecache 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 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 imagecache

Imagecache diagnostics.

```
diagnose wad worker imagecache
```

diagnose wad worker imagecache flush

Flush all blocked images in the ram disk.

```
diagnose wad worker imagecache flush
```

diagnose wad worker imagecache stats

Show statistics of blocked image cache.

```
diagnose wad worker imagecache stats
```

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 oidc

OpenID Connect diagnostics.

```
diagnose wad worker oidc
```

diagnose wad worker oidc clear-jwks

[DEBUG] Clear JWKS cache.

```
diagnose wad worker oidc clear-jwks [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker oidc refresh-server

Refresh OpenID Connect discovery servers.

```
diagnose wad worker oidc refresh-server [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker oidc servers

Show OpenID Connect servers info.

```
diagnose wad worker oidc servers [<index>]
```

Parameter	Description	Type	Size
[<index>]	Worker index or all workers if not set.	string	

diagnose wad worker oidc sessions

Show OpenID Connect sessions info.

```
diagnose wad worker oidc sessions [<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 1982](#)
- [diagnose wadbd log-show on page 1983](#)
- [diagnose wadbd restart on page 1983](#)
- [diagnose wadbd stats on page 1983](#)

diagnose wadbd clear

Remove all entries from the database.

```
diagnose wadbd clear
```

diagnose wadbd log-show

Show log of daemon

```
diagnose wadbd log-show <Disk index> <log generation> <time format>
```

Parameter	Description	Type	Size
<Disk index>	Disk index	string	
<log generation>	Log generation: default 0	string	
<time format>	Time format: 0 for human readable and 1 for raw, default 0	string	

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 1983](#)
- [diagnose waf info on page 1984](#)

diagnose waf dump

Dump WAF name table.

```
diagnose waf dump
```

diagnose waf info

Init WAF name table.

```
diagnose waf info
```

diagnose webfilter

webfilter

This topic includes the following commands:

- [diagnose webfilter bword on page 1984](#)
- [diagnose webfilter bword matchfilter on page 1984](#)
- [diagnose webfilter fortiguard on page 1985](#)
- [diagnose webfilter fortiguard cache on page 1985](#)
- [diagnose webfilter fortiguard cache dump on page 1985](#)
- [diagnose webfilter fortiguard cache obs on page 1985](#)
- [diagnose webfilter fortiguard cache prefix on page 1985](#)
- [diagnose webfilter fortiguard cache tree on page 1986](#)
- [diagnose webfilter fortiguard cache ttl on page 1986](#)
- [diagnose webfilter fortiguard override on page 1986](#)
- [diagnose webfilter fortiguard override all-admin-override on page 1986](#)
- [diagnose webfilter fortiguard override all-user-override on page 1986](#)
- [diagnose webfilter fortiguard override all-warning on page 1986](#)
- [diagnose webfilter fortiguard override obs on page 1987](#)
- [diagnose webfilter fortiguard override statistics on page 1987](#)
- [diagnose webfilter fortiguard statistics on page 1987](#)
- [diagnose webfilter fortiguard statistics flush on page 1987](#)
- [diagnose webfilter fortiguard statistics list on page 1987](#)

diagnose webfilter bword

Web banned word match filter.

```
diagnose webfilter bword
```

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

```
diagnose webfilter fortiguard
```

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 web-ui

Web user interface.

This topic includes the following commands:

- [diagnose web-ui api-cache on page 1988](#)
- [diagnose web-ui api-cache statistic on page 1988](#)
- [diagnose web-ui api-stats on page 1988](#)

- [diagnose web-ui api-stats disable on page 1989](#)
- [diagnose web-ui api-stats enable on page 1989](#)
- [diagnose web-ui api-stats list on page 1989](#)
- [diagnose web-ui api-stats reset on page 1989](#)
- [diagnose web-ui api-stats status on page 1989](#)
- [diagnose web-ui backtrace on page 1989](#)
- [diagnose web-ui backtrace clear on page 1990](#)
- [diagnose web-ui backtrace disable on page 1990](#)
- [diagnose web-ui backtrace enable on page 1990](#)
- [diagnose web-ui backtrace httpsd on page 1990](#)
- [diagnose web-ui backtrace status on page 1990](#)
- [diagnose web-ui cache on page 1990](#)
- [diagnose web-ui cache disable on page 1991](#)
- [diagnose web-ui cache enable on page 1991](#)
- [diagnose web-ui localization on page 1991](#)
- [diagnose web-ui localization disable on page 1991](#)
- [diagnose web-ui localization enable on page 1991](#)
- [diagnose web-ui next-gen-table on page 1991](#)
- [diagnose web-ui next-gen-table disable on page 1992](#)
- [diagnose web-ui next-gen-table enable on page 1992](#)

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.

```
diagnose web-ui backtrace httpsd <pid>
```

Parameter	Description	Type	Size
<pid>	Details of httpsd backtrace.	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 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 web-ui next-gen-table

Enable/disable next generation tables.

```
diagnose web-ui next-gen-table
```

diagnose web-ui next-gen-table disable

Disable next generation tables

```
diagnose web-ui next-gen-table disable
```

diagnose web-ui next-gen-table enable

Enable next generation tables.

```
diagnose web-ui next-gen-table enable
```

CLI execute commands

Use execute commands to run system commands.

This section includes syntax for the following commands:

- [execute api-user on page 1995](#)
- [execute auto-script on page 1996](#)
- [execute backup on page 1998](#)
- [execute batch on page 2012](#)
- [execute central-mgmt on page 2013](#)
- [execute cfg on page 2014](#)
- [execute clear on page 2015](#)
- [execute cli on page 2015](#)
- [execute cloud-service on page 2016](#)
- [execute config-transaction on page 2017](#)
- [execute cpu on page 2018](#)
- [execute date on page 2018](#)
- [execute device-upgrade on page 2019](#)
- [execute dhcp on page 2019](#)
- [execute dhcp6 on page 2020](#)
- [execute disconnect-admin-session on page 2021](#)
- [execute disk on page 2021](#)
- [execute enter on page 2022](#)
- [execute erase-disk on page 2022](#)
- [execute fabric-vpn on page 2023](#)
- [execute factoryreset-for-central-management on page 2024](#)
- [execute factoryreset-shutdown on page 2024](#)
- [execute factoryreset on page 2023](#)
- [execute factoryreset2 on page 2023](#)
- [execute fctems on page 2024](#)
- [execute federated-upgrade on page 2025](#)
- [execute fips on page 2027](#)
- [execute firewall on page 2028](#)
- [execute formatlogdisk on page 2029](#)
- [execute forticloud-sandbox on page 2029](#)
- [execute fortiguard-log on page 2030](#)
- [execute fortiguard-message on page 2031](#)
- [execute fortimanager on page 2031](#)
- [execute fortitoken-cloud on page 2034](#)
- [execute fortitoken-mobile on page 2036](#)

- [execute fortitoken on page 2032](#)
- [execute fsso on page 2037](#)
- [execute ha on page 2037](#)
- [execute http-view on page 2039](#)
- [execute interface on page 2039](#)
- [execute internet-service4 on page 2040](#)
- [execute internet-service6 on page 2041](#)
- [execute ipam on page 2041](#)
- [execute kmip on page 2042](#)
- [execute log on page 2043](#)
- [execute mem on page 2052](#)
- [execute nethsm on page 2053](#)
- [execute nsx on page 2060](#)
- [execute ping-options on page 2065](#)
- [execute ping on page 2061](#)
- [execute ping6-options on page 2061](#)
- [execute ping6 on page 2061](#)
- [execute policy-packet-capture on page 2069](#)
- [execute preload on page 2069](#)
- [execute private-encryption-key on page 2071](#)
- [execute reboot on page 2071](#)
- [execute report-config on page 2073](#)
- [execute report on page 2072](#)
- [execute restore on page 2073](#)
- [execute revision on page 2083](#)
- [execute send-fds-statistics on page 2084](#)
- [execute send-fmg-list on page 2085](#)
- [execute set on page 2085](#)
- [execute shutdown on page 2091](#)
- [execute speed-test-custom on page 2092](#)
- [execute speed-test-ipsec on page 2092](#)
- [execute speed-test-options on page 2092](#)
- [execute speed-test-server on page 2096](#)
- [execute speed-test on page 2091](#)
- [execute ssh-options on page 2098](#)
- [execute ssh-regen-keys on page 2099](#)
- [execute ssh on page 2096](#)
- [execute ssh6-options on page 2097](#)
- [execute ssh6 on page 2097](#)
- [execute sync-IPSec on page 2099](#)
- [execute sync-session on page 2100](#)
- [execute system on page 2100](#)
- [execute tac on page 2101](#)

- [execute telnet-options on page 2101](#)
- [execute telnet on page 2101](#)
- [execute test on page 2102](#)
- [execute time on page 2103](#)
- [execute traceroute-options on page 2103](#)
- [execute traceroute on page 2103](#)
- [execute tracert6 on page 2105](#)
- [execute upd-vd-license on page 2107](#)
- [execute update-av on page 2105](#)
- [execute update-external-resource on page 2105](#)
- [execute update-ffdb-on-demand on page 2106](#)
- [execute update-geo-ip on page 2106](#)
- [execute update-ips on page 2106](#)
- [execute update-list on page 2106](#)
- [execute update-now on page 2106](#)
- [execute update-src-vis on page 2107](#)
- [execute upload on page 2107](#)
- [execute usb-device on page 2111](#)
- [execute usb-disk on page 2112](#)
- [execute vm-license-options on page 2113](#)
- [execute vm-license on page 2113](#)
- [execute vpn on page 2116](#)
- [execute wake-on-lan on page 2124](#)
- [execute webcache on page 2125](#)
- [execute webfilter on page 2126](#)

execute api-user

api-user

This topic includes the following commands:

- [execute api-user generate-key on page 1995](#)

execute api-user generate-key

Generate key for API users.

```
execute api-user generate-key <name>
```

Parameter	Description	Type	Size
<name>	API user name.	string	

execute auto-script

auto-script

This topic includes the following commands:

- [execute auto-script backup ftp on page 1996](#)
- [execute auto-script backup tftp on page 1996](#)
- [execute auto-script delete on page 1997](#)
- [execute auto-script result on page 1997](#)
- [execute auto-script start on page 1997](#)
- [execute auto-script status on page 1997](#)
- [execute auto-script stop on page 1998](#)
- [execute auto-script stopall on page 1998](#)

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	
<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 backup

backup

This topic includes the following commands:

- [execute backup config flash on page 1999](#)
- [execute backup config ftp on page 1999](#)
- [execute backup config management-station on page 2000](#)
- [execute backup config sftp on page 2000](#)
- [execute backup config tftp on page 2000](#)
- [execute backup config usb on page 2001](#)
- [execute backup config usb-mode on page 2001](#)
- [execute backup disk alllogs ftp on page 2001](#)
- [execute backup disk alllogs tftp on page 2002](#)
- [execute backup disk alllogs usb on page 2002](#)
- [execute backup disk ipsarchives ftp on page 2002](#)
- [execute backup disk ipsarchives tftp on page 2002](#)
- [execute backup disk ipsarchives usb on page 2003](#)
- [execute backup disk log ftp on page 2003](#)
- [execute backup disk log tftp on page 2003](#)
- [execute backup disk log usb on page 2004](#)
- [execute backup full-config ftp on page 2004](#)
- [execute backup full-config sftp on page 2004](#)
- [execute backup full-config tftp on page 2005](#)
- [execute backup full-config usb on page 2005](#)

- [execute backup full-config usb-mode on page 2005](#)
- [execute backup ipsuserdefsig ftp on page 2006](#)
- [execute backup ipsuserdefsig tftp on page 2006](#)
- [execute backup memory alllogs ftp on page 2006](#)
- [execute backup memory alllogs tftp on page 2006](#)
- [execute backup memory log ftp on page 2007](#)
- [execute backup memory log tftp on page 2007](#)
- [execute backup obfuscated-config ftp on page 2007](#)
- [execute backup obfuscated-config management-station on page 2008](#)
- [execute backup obfuscated-config sftp on page 2008](#)
- [execute backup obfuscated-config tftp on page 2009](#)
- [execute backup obfuscated-config usb on page 2009](#)
- [execute backup obfuscated-full-config ftp on page 2009](#)
- [execute backup obfuscated-full-config sftp on page 2010](#)
- [execute backup obfuscated-full-config tftp on page 2010](#)
- [execute backup obfuscated-full-config usb on page 2010](#)
- [execute backup obfuscated-yaml-config ftp on page 2011](#)
- [execute backup obfuscated-yaml-config tftp on page 2011](#)
- [execute backup tls-finger-print tftp on page 2011](#)
- [execute backup yaml-config ftp on page 2012](#)
- [execute backup yaml-config tftp on page 2012](#)

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	

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> <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 config usb

Backup config file to USB disk.

```
execute backup config usb <string> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name on the USB disk.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup config usb-mode

Backup config file for USB mode.

```
execute backup config usb-mode <Enter>|<passwd>
```

Parameter	Description	Type	Size
<Enter> <passwd>	Optional password to protect the backup file.	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	

Parameter	Description	Type	Size
<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 alllogs usb

Backup all log files to USB.

```
execute backup disk alllogs usb
```

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 ipsarchives usb

Backup IPS archive file(s) to USB.

```
execute backup disk ipsarchives usb
```

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, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb	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, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb	string	

execute backup disk log usb

Backup specific log file(s) to USB.

```
execute backup disk log usb <string>
```

Parameter	Description	Type	Size
<string>	, traffic, event, virus, webfilter, ips, emailfilter, anomaly, voip, dlp, app-ctrl, waf, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb	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	

Parameter	Description	Type	Size
<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 full-config usb

Backup full config file to USB disk.

```
execute backup full-config usb <string> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name on the USB disk.	string	
<Enter> <passwd>	Optional password to protect the backup content.	string	

execute backup full-config usb-mode

Backup full config file for USB mode.

```
execute backup full-config usb-mode <Enter>|<passwd>
```

Parameter	Description	Type	Size
<Enter> <passwd>	Optional password to protect the backup file.	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, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb	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, dns, ssh, ssl, file-filter, icap, sctp-filter, forti-switch, virtual-patch, casb	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-config usb

Backup obfuscated config file to USB disk.

```
execute backup obfuscated-config usb <string> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name on the USB disk.	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-full-config usb

Backup obfuscated full config file to USB disk.

```
execute backup obfuscated-full-config usb <string> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	Make a file name on the USB disk.	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 tls-finger-print tftp

Backup config file to TFTP server.

```
execute backup tls-finger-print 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 2013](#)
- [execute batch lastlog on page 2013](#)
- [execute batch start on page 2013](#)
- [execute batch status on page 2013](#)

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 2013](#)
- [execute central-mgmt set-mgmt-id on page 2014](#)
- [execute central-mgmt unregister-device on page 2014](#)

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 2014](#)
- [execute cfg save on page 2015](#)

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 2015](#)

execute clear system arp table

Clear system ARP table.

```
execute clear system arp table
```

execute cli

cli

This topic includes the following commands:

- [execute cli check-template-status on page 2015](#)
- [execute cli status-msg-only on page 2016](#)

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 2016](#)
- [execute cloud-service list on page 2016](#)
- [execute cloud-service manual-gen-jwt-as-token on page 2017](#)

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>
```

Parameter	Description	Type	Size
<string>	keyid.	string	

execute config-transaction

config-transaction

This topic includes the following commands:

- [execute config-transaction abort on page 2017](#)
- [execute config-transaction commit on page 2017](#)
- [execute config-transaction start on page 2017](#)

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 2018](#)
- [execute cpu show on page 2018](#)

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 2019](#)
- [execute device-upgrade immediate on page 2019](#)

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 2020](#)
- [execute dhcp lease-list on page 2020](#)

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 2021](#)
- [execute dhcp6 lease-list on page 2021](#)

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 2022](#)
- [execute disk list on page 2022](#)
- [execute disk scan on page 2022](#)

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 fabric-vpn

fabric-vpn

This topic includes the following commands:

- [execute fabric-vpn flush-setup on page 2023](#)
- [execute fabric-vpn update-setup on page 2023](#)

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 2025](#)
- [execute fctems unverify on page 2025](#)
- [execute fctems verify on page 2025](#)

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 2026](#)
- [execute federated-upgrade initialize on page 2026](#)
- [execute federated-upgrade quick-fortigate-upgrade on page 2026](#)
- [execute federated-upgrade quick-full-upgrade on page 2026](#)
- [execute federated-upgrade restart on page 2027](#)
- [execute federated-upgrade safe-cancel on page 2027](#)

- [execute federated-upgrade status on page 2027](#)

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	
<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 2028](#)
- [execute fips tftp-test-vectors on page 2028](#)

execute fips tftp-drbg-entropy-source

tftp files and generate drbg entropy source samples

```
execute fips tftp-drbg-entropy-source <ip> <dir> <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	

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 2028](#)
- [execute firewall ssh generate local-key on page 2029](#)

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 forticloud-sandbox

forticloud-sandbox

This topic includes the following commands:

- [execute forticloud-sandbox region on page 2029](#)
- [execute forticloud-sandbox update on page 2029](#)

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 2030](#)
- [execute fortiguard-log migration on page 2030](#)
- [execute fortiguard-log update on page 2030](#)

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 FortiProxy 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 2031](#)
- [execute fortiguard-message info on page 2031](#)
- [execute fortiguard-message update on page 2031](#)

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 2032](#)
- [execute fortimanager register on page 2032](#)

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 2032](#)
- [execute fortitoken import ftp on page 2033](#)
- [execute fortitoken import tftp on page 2033](#)
- [execute fortitoken import usb on page 2033](#)
- [execute fortitoken import-sn-file on page 2033](#)
- [execute fortitoken sync on page 2034](#)

execute fortitoken activate

Activate FortiToken(s) with FortiGuard.

```
execute fortitoken activate <id>
```

Parameter	Description	Type	Size
<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 2034](#)
- [execute fortitoken-cloud new on page 2035](#)
- [execute fortitoken-cloud show on page 2035](#)
- [execute fortitoken-cloud sync on page 2035](#)
- [execute fortitoken-cloud trial on page 2035](#)
- [execute fortitoken-cloud update on page 2035](#)

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 FortiProxy.

```
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 2036](#)
- [execute fortitoken-mobile poll on page 2036](#)
- [execute fortitoken-mobile provision on page 2036](#)
- [execute fortitoken-mobile renew on page 2036](#)

execute fortitoken-mobile import

Import a list of tokens from FortiGuard to the FortiProxy 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 2037](#)

execute fsso refresh

Refresh FSSO groups.

```
execute fsso refresh
```

execute ha

ha

This topic includes the following commands:

- [execute ha disconnect on page 2037](#)
- [execute ha failover set on page 2038](#)
- [execute ha failover status on page 2038](#)
- [execute ha failover unset on page 2038](#)
- [execute ha manage on page 2038](#)
- [execute ha synchronize on page 2039](#)

execute ha disconnect

Disconnect from HA cluster.

```
execute ha disconnect <string>
```

Parameter	Description	Type	Size
<string>	Serial number.	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>
```

Parameter	Description	Type	Size
<string>	HA cluster index.	string	

execute ha synchronize

HA synchronize commands.

```
execute ha synchronize <string>
```

Parameter	Description	Type	Size
<string>	File type.	string	

execute http-view

http-view

This topic includes the following commands:

- [execute http-view report on page 2039](#)

execute http-view report

Report latest HTTP/S traffic statistics

```
execute http-view report <type> <top n> <minutes>
```

Parameter	Description	Type	Size
<type>	Numeric, report type	string	
<top n>	Number of top entries to display (5 - 100)	string	
<minutes>	Duration of recent time to report (1 - Max-Configured)	string	

execute interface

interface

This topic includes the following commands:

- [execute interface dhcp6client-renew on page 2040](#)
- [execute interface dhcpclient-renew on page 2040](#)
- [execute interface pppoe-reconnect on page 2040](#)

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 2041](#)

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 2041](#)

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 2041](#)

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 kmip

kmip

This topic includes the following commands:

- [execute kmip create on page 2042](#)
- [execute kmip destroy on page 2042](#)
- [execute kmip get on page 2043](#)
- [execute kmip locate on page 2043](#)
- [execute kmip rekey on page 2043](#)

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 2044](#)
- [execute log backup local on page 2045](#)
- [execute log backup tftp on page 2045](#)
- [execute log delete on page 2045](#)
- [execute log delete-all on page 2045](#)

- [execute log detail on page 2046](#)
- [execute log display on page 2046](#)
- [execute log filter category on page 2046](#)
- [execute log filter device on page 2046](#)
- [execute log filter dump on page 2046](#)
- [execute log filter field on page 2047](#)
- [execute log filter free-style on page 2047](#)
- [execute log filter ha-member on page 2047](#)
- [execute log filter local-search-mode on page 2048](#)
- [execute log filter max-checklines on page 2048](#)
- [execute log filter pre-fetch-pages on page 2048](#)
- [execute log filter reset on page 2048](#)
- [execute log filter start-line on page 2049](#)
- [execute log filter view-lines on page 2049](#)
- [execute log flush-cache on page 2049](#)
- [execute log flush-cache-all on page 2049](#)
- [execute log fortianalyzer manual-failover on page 2049](#)
- [execute log fortianalyzer test-connectivity on page 2050](#)
- [execute log fortianalyzer-cloud test-connectivity on page 2050](#)
- [execute log fortianalyzer2 manual-failover on page 2050](#)
- [execute log fortianalyzer3 manual-failover on page 2050](#)
- [execute log fortiguard test-connectivity on page 2050](#)
- [execute log list on page 2050](#)
- [execute log raw-backup ftp on page 2051](#)
- [execute log raw-backup tftp on page 2051](#)
- [execute log restore on page 2051](#)
- [execute log roll on page 2051](#)
- [execute log shift-time on page 2052](#)
- [execute log upload on page 2052](#)
- [execute log upload-progress on page 2052](#)

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 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 2052](#)

execute mem add

Online new memory blocks.

```
execute mem add
```


execute nethsm

nethsm

This topic includes the following commands:

- [execute nethsm primus clear-pkcs-provider-log on page 2053](#)
- [execute nethsm primus clear-primus-log on page 2054](#)
- [execute nethsm primus delete-object on page 2054](#)
- [execute nethsm primus dump-pkcs-provider-log on page 2054](#)
- [execute nethsm primus dump-primus-log on page 2054](#)
- [execute nethsm primus inspect-primus-library-info on page 2054](#)
- [execute nethsm primus list-objects on page 2054](#)
- [execute nethsm primus upload-primus-cfg on page 2055](#)
- [execute nethsm primus upload-primus-cfg-raw on page 2055](#)
- [execute nethsm safenet clear-log on page 2055](#)
- [execute nethsm safenet client-cert-create on page 2055](#)
- [execute nethsm safenet client-cert-export ftp on page 2055](#)
- [execute nethsm safenet client-cert-export tftp on page 2056](#)
- [execute nethsm safenet client-cert-show on page 2056](#)
- [execute nethsm safenet config-export ftp on page 2056](#)
- [execute nethsm safenet config-export tftp on page 2057](#)
- [execute nethsm safenet config-import ftp on page 2057](#)
- [execute nethsm safenet config-import tftp on page 2057](#)
- [execute nethsm safenet config-show on page 2057](#)
- [execute nethsm safenet diagnose on page 2058](#)
- [execute nethsm safenet hagroup-add on page 2058](#)
- [execute nethsm safenet hagroup-del on page 2058](#)
- [execute nethsm safenet hagroup-list on page 2058](#)
- [execute nethsm safenet register on page 2058](#)
- [execute nethsm safenet reset on page 2059](#)
- [execute nethsm safenet restore-conf on page 2059](#)
- [execute nethsm safenet set-conf-opt on page 2059](#)
- [execute nethsm safenet show-log on page 2059](#)
- [execute nethsm safenet status on page 2059](#)
- [execute nethsm safenet unregister on page 2060](#)

execute nethsm primus clear-pkcs-provider-log

Clear logs from /var/log/pkcs11.log, generated by pkcs11.so, the OpenSSL provider.

```
execute nethsm primus clear-pkcs-provider-log
```

execute nethsm primus clear-primus-log

Clear logs from /var/log/primus.log, generated by libprimusP11.so.

```
execute nethsm primus clear-primus-log
```

execute nethsm primus delete-object

Delete Hardware Security Module object(s).

```
execute nethsm primus delete-object <label>
```

Parameter	Description	Type	Size
<label>	Label of the HSM object(s) to delete.	string	

execute nethsm primus dump-pkcs-provider-log

Dump logs from /var/log/pkcs11.log, generated by pkcs11.so, the OpenSSL provider.

```
execute nethsm primus dump-pkcs-provider-log
```

execute nethsm primus dump-primus-log

Dump logs from /var/log/primus.log, generated by libprimusP11.so.

```
execute nethsm primus dump-primus-log
```

execute nethsm primus inspect-primus-library-info

Display information about the integrated libprimusP11.so library.

```
execute nethsm primus inspect-primus-library-info
```

execute nethsm primus list-objects

List Hardware Security Module objects.

```
execute nethsm primus list-objects
```

execute nethsm primus upload-primus-cfg

Upload nethsm primus.cfg file.

```
execute nethsm primus upload-primus-cfg <filename> <tftp server>
```

Parameter	Description	Type	Size
<filename>	File name on the TFTP server.	string	
<tftp server>	TFTP server IP or FQDN.	string	

execute nethsm primus upload-primus-cfg-raw

Upload nethsm primus.cfg file.

```
execute nethsm primus upload-primus-cfg-raw <filename> <tftp server>
```

Parameter	Description	Type	Size
<filename>	File name on the TFTP server.	string	
<tftp server>	TFTP server IP or FQDN.	string	

execute nethsm safenet clear-log

Clear NETHSM log.

```
execute nethsm safenet clear-log
```

execute nethsm safenet client-cert-create

(Re)Create client certificate.

```
execute nethsm safenet client-cert-create <string>
```

Parameter	Description	Type	Size
<string>	Country name (e.g. Canada) or country code (e.g. ca).	string	

execute nethsm safenet client-cert-export ftp

Export client certificate over FTP

```
execute nethsm safenet client-cert-export ftp <ftp server>[:ftp port] <remote-path> <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<ftp server>[:ftp port]	FTP server IP, can be attached with port.	string	
<remote-path>	FTP remote directory.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute nethsm safenet client-cert-export tftp

Export client certificate over TFTP

```
execute nethsm safenet client-cert-export tftp <ip>
```

Parameter	Description	Type	Size
<ip>	IP address of TFTP server.	string	

execute nethsm safenet client-cert-show

Display client certificate

```
execute nethsm safenet client-cert-show
```

execute nethsm safenet config-export ftp

Import nethsm config from a FTP server.

```
execute nethsm safenet config-export ftp <ip>[:ftp port] <remote-path> <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<ip>[:ftp port]	FTP server IP, can also include port.	string	
<remote-path>	FTP remote directory.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute nethsm safenet config-export tftp

Export nethsm config over TFTP

```
execute nethsm safenet config-export tftp <ip>
```

Parameter	Description	Type	Size
<ip>	IP address of TFTP server.	string	

execute nethsm safenet config-import ftp

Export nethsm config over FTP

```
execute nethsm safenet config-import ftp <string> <ftp server>[:ftp port] <Enter>|<user> <passwd>
```

Parameter	Description	Type	Size
<string>	File name on the FTP server.	string	
<ftp server>[:ftp port]	FTP server IP, can also include port.	string	
<Enter> <user>	FTP username may be needed.	string	
<passwd>	FTP password.	string	

execute nethsm safenet config-import tftp

Import nethsm config from a TFTP server.

```
execute nethsm safenet config-import tftp <string> <ip>
```

Parameter	Description	Type	Size
<string>	File name on the TFTP server.	string	
<ip>	IP address of TFTP server.	string	

execute nethsm safenet config-show

Display nethsm config

```
execute nethsm safenet config-show
```

execute nethsm safenet diagnose

Partition diagnose.

```
execute nethsm safenet diagnose
```

execute nethsm safenet hagroup-add

Add HA group.

```
execute nethsm safenet hagroup-add <hagroup>
```

Parameter	Description	Type	Size
<hagroup>	HSM HA group name.	string	

execute nethsm safenet hagroup-del

Delete HA group.

```
execute nethsm safenet hagroup-del <hagroup>
```

Parameter	Description	Type	Size
<hagroup>	HSM HA group name.	string	

execute nethsm safenet hagroup-list

List HA group.

```
execute nethsm safenet hagroup-list <hagroup>
```

Parameter	Description	Type	Size
<hagroup>	HSM HA group name.	string	

execute nethsm safenet register

Register to network HSM server.

```
execute nethsm safenet register <server>
```

Parameter	Description	Type	Size
<server>	HSM server name.	string	

execute nethsm safenet reset

Erase all NETHSM config.

```
execute nethsm safenet reset
```

execute nethsm safenet restore-conf

Restore NETHSM config.

```
execute nethsm safenet restore-conf
```

execute nethsm safenet set-conf-opt

Set NETHSM config option.

```
execute nethsm safenet set-conf-opt
```

execute nethsm safenet show-log

Show NETHSM log.

```
execute nethsm safenet show-log
```

execute nethsm safenet status

Client status.

```
execute nethsm safenet status <server>
```

Parameter	Description	Type	Size
<server>	HSM server name.	string	

execute nethsm safenet unregister

Unregister from network HSM server.

```
execute nethsm safenet unregister <server>
```

Parameter	Description	Type	Size
<server>	HSM server name.	string	

execute nsx

nsx

This topic includes the following commands:

- [execute nsx group delete on page 2060](#)
- [execute nsx group import on page 2060](#)
- [execute nsx group list on page 2061](#)

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 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 2062](#)
- [execute ping6-options data-size on page 2062](#)
- [execute ping6-options interface on page 2062](#)
- [execute ping6-options interval on page 2062](#)
- [execute ping6-options pattern on page 2063](#)
- [execute ping6-options repeat-count on page 2063](#)

- [execute ping6-options reset on page 2063](#)
- [execute ping6-options source6 on page 2063](#)
- [execute ping6-options timeout on page 2064](#)
- [execute ping6-options tos on page 2064](#)
- [execute ping6-options ttl on page 2064](#)
- [execute ping6-options validate-reply on page 2064](#)
- [execute ping6-options view-settings on page 2064](#)

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 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 ping-options

ping-options

This topic includes the following commands:

- [execute ping-options adaptive-ping on page 2065](#)
- [execute ping-options data-size on page 2065](#)
- [execute ping-options df-bit on page 2066](#)
- [execute ping-options interface on page 2066](#)
- [execute ping-options interval on page 2066](#)
- [execute ping-options pattern on page 2066](#)
- [execute ping-options repeat-count on page 2067](#)
- [execute ping-options reset on page 2067](#)
- [execute ping-options source on page 2067](#)
- [execute ping-options timeout on page 2067](#)
- [execute ping-options tos on page 2067](#)
- [execute ping-options ttl on page 2068](#)
- [execute ping-options use-sdwan on page 2068](#)
- [execute ping-options validate-reply on page 2068](#)
- [execute ping-options view-settings on page 2068](#)

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 policy-packet-capture

policy-packet-capture

This topic includes the following commands:

- [execute policy-packet-capture delete-all on page 2069](#)

execute policy-packet-capture delete-all

Delete all captured packet.

```
execute policy-packet-capture delete-all
```

execute preload

preload

This topic includes the following commands:

- [execute preload http-transaction-log disable on page 2069](#)
- [execute preload http-transaction-log enable on page 2069](#)
- [execute preload list on page 2070](#)
- [execute preload show-log on page 2070](#)
- [execute preload url on page 2070](#)
- [execute preload url-delete on page 2070](#)

execute preload http-transaction-log disable

Disables preload http transaction log

```
execute preload http-transaction-log disable
```

execute preload http-transaction-log enable

Enables preload http transaction log

```
execute preload http-transaction-log enable
```

execute preload list

Lists scheduled URLs

```
execute preload list
```

execute preload show-log

Show log of last preload runs

```
execute preload show-log
```

execute preload url

Schedule a new preload operation for a URL

```
execute preload url <url> <depth> <ignore-robots> <at_time> <repeat_after> <repetitions> <user-agent> <user>
```

Parameter	Description	Type	Size
<url>	URL to preload	string	
<depth>	Depth of preload. Defaults to 0	string	
<ignore-robots>	Ignore robots.txt rules. Defaults to disable[0]	string	
<at_time>	HHH:MM. HHH - hours from now [0-672], MM - Minutes from now [0-59]. Default is 0:00	string	
<repeat_after>	HHH:MM. HHH - hours from now [0-168], MM - Minutes from now [0-59]. Default is max	string	
<repetitions>	End after this many repetitions. Defaulted to 1.	string	
<user-agent>	Specify client type (Free text) to identify as	string	
<user>	Specify user (Password will be on separate prompt)	string	

execute preload url-delete

Deletes scheduled preload operation for the URL

```
execute preload url-delete <url-delete>
```

Parameter	Description	Type	Size
<url-delete>	Delete scheduled URLfor preload	string	

execute private-encryption-key

private-encryption-key

This topic includes the following commands:

- [execute private-encryption-key sample on page 2071](#)
- [execute private-encryption-key verify on page 2071](#)

execute private-encryption-key sample

Generate base64 clear text and its HMAC signature encrypted by private key.

```
execute private-encryption-key sample
```

execute private-encryption-key verify

Verify if the input base64 HMAC is encrypted by private key.

```
execute private-encryption-key verify <string>
```

Parameter	Description	Type	Size
<string>	base64-clear-text.	string	

execute reboot

Reboot now.

```
execute reboot <comment> <string>
```

Parameter	Description	Type	Size
<comment>	comment	string	
<string>	Reboot comments.	string	

execute report

report

This topic includes the following commands:

- [execute report flush-cache on page 2072](#)
- [execute report recreate-db on page 2072](#)
- [execute report run on page 2072](#)
- [execute report sandbox-status on page 2072](#)

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 2073](#)

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 2074](#)
- [execute restore av tftp on page 2074](#)
- [execute restore config dhcp on page 2075](#)
- [execute restore config flash on page 2075](#)
- [execute restore config ftp on page 2075](#)
- [execute restore config management-station normal on page 2076](#)
- [execute restore config management-station script on page 2076](#)
- [execute restore config management-station template on page 2076](#)
- [execute restore config tftp on page 2076](#)
- [execute restore config usb on page 2077](#)
- [execute restore config usb-mode on page 2077](#)
- [execute restore image flash on page 2077](#)
- [execute restore image ftp on page 2077](#)
- [execute restore image management-station on page 2078](#)

- [execute restore image tftp on page 2078](#)
- [execute restore image url on page 2078](#)
- [execute restore image usb on page 2079](#)
- [execute restore ips ftp on page 2079](#)
- [execute restore ips tftp on page 2079](#)
- [execute restore ipsuserdefsig ftp on page 2079](#)
- [execute restore ipsuserdefsig tftp on page 2080](#)
- [execute restore manual-license ftp on page 2080](#)
- [execute restore manual-license tftp on page 2080](#)
- [execute restore other-objects ftp on page 2081](#)
- [execute restore other-objects tftp on page 2081](#)
- [execute restore script ftp on page 2081](#)
- [execute restore script lastlog on page 2082](#)
- [execute restore script scp on page 2082](#)
- [execute restore script tftp on page 2082](#)
- [execute restore vmlicense ftp on page 2083](#)
- [execute restore vmlicense tftp on page 2083](#)

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	

Parameter	Description	Type	Size
<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 config usb

Load config file from USB disk to firewall.

```
execute restore config usb <string> <Enter>|<passwd>
```

Parameter	Description	Type	Size
<string>	File name on USB disk.	string	
<Enter> <passwd>	Password may be needed to restore.	string	

execute restore config usb-mode

Load config file from USB disk and reboot.

```
execute restore config usb-mode <Enter>|<passwd>
```

Parameter	Description	Type	Size
<Enter> <passwd>	Optional password to protect.	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 image usb

Restore image from USB disk.

```
execute restore image usb <string>
```

Parameter	Description	Type	Size
<string>	Image file name on the USB disk.	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 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	
<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 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 2083](#)
- [execute revision delete image on page 2084](#)
- [execute revision list config on page 2084](#)
- [execute revision list image on page 2084](#)

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 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 2086](#)
- [execute set system session filter clear dport on page 2086](#)
- [execute set system session filter clear dst on page 2086](#)
- [execute set system session filter clear duration on page 2086](#)
- [execute set system session filter clear expire on page 2086](#)
- [execute set system session filter clear policy on page 2086](#)
- [execute set system session filter clear proto on page 2087](#)
- [execute set system session filter clear sport on page 2087](#)
- [execute set system session filter clear src on page 2087](#)
- [execute set system session filter clear vd on page 2087](#)
- [execute set system session filter dport on page 2087](#)
- [execute set system session filter dst on page 2087](#)
- [execute set system session filter duration on page 2088](#)
- [execute set system session filter expire on page 2088](#)
- [execute set system session filter list on page 2088](#)
- [execute set system session filter negate dport on page 2088](#)
- [execute set system session filter negate dst on page 2088](#)
- [execute set system session filter negate duration on page 2089](#)
- [execute set system session filter negate expire on page 2089](#)
- [execute set system session filter negate policy on page 2089](#)
- [execute set system session filter negate proto on page 2089](#)
- [execute set system session filter negate sport on page 2089](#)
- [execute set system session filter negate src on page 2089](#)
- [execute set system session filter negate vd on page 2090](#)
- [execute set system session filter policy on page 2090](#)
- [execute set system session filter proto on page 2090](#)
- [execute set system session filter sport on page 2090](#)
- [execute set system session filter src on page 2090](#)
- [execute set system session filter vd on page 2091](#)

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>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	

execute set system session filter dst

Destination IP address.

```
execute set system session filter dst <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Destination IP (from).	string	

execute set system session filter duration

duration

```
execute set system session filter duration <xxx>
```

Parameter	Description	Type	Size
<xxx>	Duration (from).	string	

execute set system session filter expire

expire

```
execute set system session filter expire <xxx>
```

Parameter	Description	Type	Size
<xxx>	Expire (from).	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>
```

Parameter	Description	Type	Size
<xxx>	Policy ID (from).	string	

execute set system session filter proto

Protocol number.

```
execute set system session filter proto <xx>
```

Parameter	Description	Type	Size
<xx>	<0-255> (from).	string	

execute set system session filter sport

Source port.

```
execute set system session filter sport <xxxx>
```

Parameter	Description	Type	Size
<xxxx>	<0-65535> (from).	string	

execute set system session filter src

Source IP address.

```
execute set system session filter src <xxx.xxx.xxx.xxx>
```

Parameter	Description	Type	Size
<xxx.xxx.xxx.xxx>	Source IP (from).	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 2093](#)
- [execute speed-test-options burst on page 2093](#)
- [execute speed-test-options ctrl-port on page 2093](#)
- [execute speed-test-options duration on page 2093](#)
- [execute speed-test-options get-token on page 2094](#)
- [execute speed-test-options max-down on page 2094](#)
- [execute speed-test-options max-up on page 2094](#)
- [execute speed-test-options protocol on page 2094](#)
- [execute speed-test-options reset on page 2095](#)
- [execute speed-test-options reset-token on page 2095](#)
- [execute speed-test-options server-port on page 2095](#)
- [execute speed-test-options set-shaper on page 2095](#)

- [execute speed-test-options show on page 2095](#)
- [execute speed-test-options tos on page 2096](#)

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 2096](#)
- [execute speed-test-server list on page 2096](#)

execute speed-test-server download

Download server list from FortiProxy 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 2097](#)
- [execute ssh6-options reset on page 2097](#)
- [execute ssh6-options source6 on page 2098](#)
- [execute ssh6-options view-settings on page 2098](#)

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 2098](#)
- [execute ssh-options reset on page 2099](#)
- [execute ssh-options source on page 2099](#)
- [execute ssh-options view-settings on page 2099](#)

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 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 2100](#)
- [execute system fortisandbox test-alternative-connectivity on page 2100](#)
- [execute system fortisandbox test-primary-connectivity on page 2100](#)

execute system custom-language import

Import a custom language from the TFTP server.

```
execute system custom-language import <string>
```

Parameter	Description	Type	Size
<string>	The language name.	string	

execute system fortisandbox test-alternative-connectivity

Query alternative FortiSandbox connection status.

```
execute system fortisandbox test-alternative-connectivity
```

execute system fortisandbox test-primary-connectivity

Query FortiSandbox connection status.

```
execute system fortisandbox test-primary-connectivity
```


execute tac

tac

This topic includes the following commands:

- [execute tac report on page 2101](#)

execute tac report

Debug report.

```
execute tac report
```



This command displays all memory usage of WAD processes, which can spike CPU usage or block the CLI for seconds.

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 2102](#)
- [execute telnet-options reset on page 2102](#)
- [execute telnet-options source on page 2102](#)
- [execute telnet-options view-settings on page 2102](#)

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 2103](#)

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 2104](#)
- [execute traceroute-options queries on page 2104](#)
- [execute traceroute-options reset on page 2104](#)
- [execute traceroute-options source on page 2104](#)
- [execute traceroute-options use-sdwan on page 2105](#)
- [execute traceroute-options view-settings on page 2105](#)

execute traceroute-options device

Auto | <ifname>.

```
execute traceroute-options device <string>
```

Parameter	Description	Type	Size
<string>	Auto <ifname>	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 tracert6

Traceroute for IPv6.

```
execute tracert6
```

execute update-av

Update AV engine/definitions.

```
execute update-av
```

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-list

Download update server list.

```
execute update-list
```

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 2107](#)
- [execute upload config tftp on page 2108](#)
- [execute upload config usb on page 2108](#)
- [execute upload fortinbi-installer cloud on page 2108](#)
- [execute upload fortinbi-installer tftp on page 2109](#)
- [execute upload fortinbi-isolator-image cloud on page 2109](#)
- [execute upload fortinbi-isolator-image tftp on page 2109](#)
- [execute upload image ftp on page 2109](#)
- [execute upload image tftp on page 2110](#)
- [execute upload image usb on page 2110](#)
- [execute upload report-img ftp on page 2110](#)
- [execute upload report-img tftp on page 2111](#)

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 config usb

Load config from USB to local disk.

```
execute upload config usb <string> <comment>
```

Parameter	Description	Type	Size
<string>	File name on USB disk.	string	
<comment>	comments	string	

execute upload fortinbi-installer cloud

Upload the FortiNBI installer from cloud.


```
execute upload fortinbi-installer cloud
```

execute upload fortinbi-installer tftp

Upload the FortiNBI installer from a TFTP server.

```
execute upload fortinbi-installer 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 upload fortinbi-isolator-image cloud

Upload the FortiNBI isolator image from cloud.

```
execute upload fortinbi-isolator-image cloud
```

execute upload fortinbi-isolator-image tftp

Upload the FortiNBI isolator image from a TFTP server.

```
execute upload fortinbi-isolator-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 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	

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 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 image usb

Load image from USB to local disk.

```
execute upload image usb <string> <comment>
```

Parameter	Description	Type	Size
<string>	File name on USB disk.	string	
<comment>	comments	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	

Parameter	Description	Type	Size
<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 usb-device

usb-device

This topic includes the following commands:

- [execute usb-device disconnect on page 2111](#)
- [execute usb-device list on page 2111](#)
- [execute usb-device modeswitch on page 2112](#)

execute usb-device disconnect

Disconnect a USB device.

```
execute usb-device disconnect
```

execute usb-device list

Display the lists of the USB device.

```
execute usb-device list
```

execute usb-device modeswitch

Perform usb device mode switch

```
execute usb-device modeswitch <argument string>
```

Parameter	Description	Type	Size
<argument string>	usb_modeswitch arguments. e.g: usb_modeswitch '-v 0x12d1 -p 0x1f01 -V 0x12d1 -P 0x14dc'	string	

execute usb-disk

usb-disk

This topic includes the following commands:

- [execute usb-disk delete on page 2112](#)
- [execute usb-disk eject on page 2112](#)
- [execute usb-disk format on page 2113](#)
- [execute usb-disk list on page 2113](#)
- [execute usb-disk rename on page 2113](#)

execute usb-disk delete

Delete file from the USB disk.

```
execute usb-disk delete <filename>
```

Parameter	Description	Type	Size
<filename>	File in the USB disk.	string	

execute usb-disk eject

Eject the USB disk.

```
execute usb-disk eject
```

execute usb-disk format

Format the USB disk.

```
execute usb-disk format
```

execute usb-disk list

Display the contents of the USB disk.

```
execute usb-disk list
```

execute usb-disk rename

Rename file in the USB disk.

```
execute usb-disk rename <old> <new>
```

Parameter	Description	Type	Size
<old>	Old file in the USB disk.	string	
<new>	New file in the USB disk.	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 2114](#)
- [execute vm-license-options account-password on page 2114](#)
- [execute vm-license-options count on page 2114](#)
- [execute vm-license-options government on page 2115](#)
- [execute vm-license-options interval on page 2115](#)
- [execute vm-license-options proxy on page 2115](#)
- [execute vm-license-options reset on page 2115](#)
- [execute vm-license-options show on page 2115](#)
- [execute vm-license-options token on page 2116](#)

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 2117](#)
- [execute vpn certificate ca import auto on page 2117](#)
- [execute vpn certificate ca import bundle on page 2117](#)
- [execute vpn certificate ca import est on page 2117](#)
- [execute vpn certificate ca import tftp on page 2118](#)
- [execute vpn certificate crl import auto on page 2118](#)
- [execute vpn certificate ems_ca import tftp on page 2118](#)
- [execute vpn certificate hsm primus generate ec on page 2118](#)
- [execute vpn certificate hsm primus generate rsa on page 2119](#)
- [execute vpn certificate hsm primus load-key on page 2119](#)
- [execute vpn certificate hsm safenet generate rsa on page 2119](#)
- [execute vpn certificate hsm-local gch-get-versions on page 2119](#)
- [execute vpn certificate hsm-local status on page 2120](#)
- [execute vpn certificate hsm-local verify on page 2120](#)
- [execute vpn certificate local export tftp on page 2120](#)
- [execute vpn certificate local generate cmp-ec on page 2120](#)
- [execute vpn certificate local generate cmp-rsa on page 2120](#)
- [execute vpn certificate local generate default-gui-mgmt-cert on page 2121](#)
- [execute vpn certificate local generate default-ssl-ca on page 2121](#)
- [execute vpn certificate local generate default-ssl-ca-untrusted on page 2121](#)
- [execute vpn certificate local generate default-ssl-key-certs on page 2121](#)
- [execute vpn certificate local generate default-ssl-serv-key on page 2122](#)
- [execute vpn certificate local generate ec on page 2122](#)
- [execute vpn certificate local generate est on page 2122](#)
- [execute vpn certificate local generate rsa on page 2122](#)
- [execute vpn certificate local import tftp on page 2123](#)

- [execute vpn certificate local verify on page 2123](#)
- [execute vpn certificate remote export tftp on page 2123](#)
- [execute vpn certificate remote import tftp on page 2123](#)
- [execute vpn ipsec tunnel down on page 2124](#)
- [execute vpn ipsec tunnel up on page 2124](#)

execute vpn certificate ca export tftp

Export CA certificate to a TFTP server.

```
execute vpn certificate ca export tftp <string>
```

Parameter	Description	Type	Size
<string>	CA certificate name.	string	

execute vpn certificate ca import auto

Import CA certificate via SCEP.

```
execute vpn certificate ca import auto <string>
```

Parameter	Description	Type	Size
<string>	URL of the CA server.	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>
```

Parameter	Description	Type	Size
<string>	URL of the CA server. (e.g. https://example.com:1234).	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 primus generate ec

Generate a Primus HSM elliptic curve certificate request.

```
execute vpn certificate hsm primus generate ec <string>
```

Parameter	Description	Type	Size
<string>	Hardware Security Module partition name.	string	

execute vpn certificate hsm primus generate rsa

Generate a Primus HSM RSA certificate request.

```
execute vpn certificate hsm primus generate rsa <string>
```

Parameter	Description	Type	Size
<string>	Hardware Security Module partition name.	string	

execute vpn certificate hsm primus load-key

Try to load in a certificate from the Primus HSM.

```
execute vpn certificate hsm primus load-key <string>
```

Parameter	Description	Type	Size
<string>	Local and Hardware Security Module key name.	string	

execute vpn certificate hsm safenet generate rsa

Generate a SafeNet HSM RSA certificate request.

```
execute vpn certificate hsm safenet generate rsa <string>
```

Parameter	Description	Type	Size
<string>	HSM slot name.	string	

execute vpn certificate hsm-local gch-get-versions

List available crypto-key-versions.

```
execute vpn certificate hsm-local gch-get-versions <string>
```

Parameter	Description	Type	Size
<string>	hsm-local certificate name.	string	

execute vpn certificate hsm-local status

Status check for an hsm-local certificate.

```
execute vpn certificate hsm-local status <string>
```

Parameter	Description	Type	Size
<string>	hsm-local certificate name.	string	

execute vpn certificate hsm-local verify

Verify between hsm-local certificate and its private key.

```
execute vpn certificate hsm-local verify <string>
```

Parameter	Description	Type	Size
<string>	hsm-local certificate name.	string	

execute vpn certificate local export tftp

Export local certificate or certificate request to a TFTP server.

```
execute vpn certificate local export tftp <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	

execute vpn certificate local generate cmp-ec

Generate a ECDSA certificate request over CMPv2.

```
execute vpn certificate local generate cmp-ec <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	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>
```

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	

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>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	

execute vpn certificate local generate est

Generate an certificate via Enrollment over Secure Transport.

```
execute vpn certificate local generate est <string>
```

Parameter	Description	Type	Size
<string>	Local certificate name.	string	

execute vpn certificate local generate rsa

Generate a RSA certificate request.

```
execute vpn certificate local generate rsa <string> <number> <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	

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>
```

Parameter	Description	Type	Size
<string>	REMOTE certificate name.	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 ipsec tunnel down

Shut down the specified IPsec tunnel.

```
execute vpn ipsec tunnel down <phase1>
```

Parameter	Description	Type	Size
<phase1>	Phase1 name.	string	

execute vpn ipsec tunnel up

Activate the specified IPsec tunnel.

```
execute vpn ipsec tunnel up <phase1>
```

Parameter	Description	Type	Size
<phase1>	Phase1 name.	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	

Parameter	Description	Type	Size
<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 2125](#)
- [execute webcache delete simple-string on page 2125](#)
- [execute webcache delete status on page 2125](#)
- [execute webcache delete wildcard on page 2126](#)

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 2126](#)

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	



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.