

CLI Reference

FortiOS 7.0.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



July 20, 2021

FortiOS 7.0.1 CLI Reference

01-701-709094-20210720

TABLE OF CONTENTS

Change Log	17
FortiOS CLI reference	18
Creation of the CLI reference	18
Availability of commands and options	18
CLI configuration commands	20
alertemail	21
config alertemail setting	21
antivirus	28
config antivirus settings	28
config antivirus quarantine	29
config antivirus profile	34
application	64
config application name	64
config application custom	66
config application rule-settings	67
config application list	67
config application group	75
authentication	77
config authentication scheme	77
config authentication rule	79
config authentication setting	81
certificate	84
config certificate ca	84
config certificate remote	85
config certificate local	86
config certificate crl	89
dlp	92
config dlp filepattern	92
config dlp sensitivity	95
config dlp sensor	95
dnsfilter	101
config dnsfilter domain-filter	101
config dnsfilter profile	102
emailfilter	107
config emailfilter bword	107
config emailfilter block-allow-list	109
config emailfilter mheader	111
config emailfilter dnsbl	112
config emailfilter iptrust	113
config emailfilter profile	114
config emailfilter fortishield	121
config emailfilter options	122
endpoint-control	123
config endpoint-control fitems	123

extender	127
config extender sys-info	127
config extender extender-info	127
config extender modem-status	128
config extender lte-carrier-list	128
config extender lte-carrier-by-mcc-mnc	128
extender-controller	129
config extender-controller dataplan	129
config extender-controller extender	131
file-filter	139
config file-filter profile	139
firewall	142
config firewall address	144
config firewall multicast-address	148
config firewall address6-template	150
config firewall address6	151
config firewall multicast-address6	154
config firewall addrgrp	155
config firewall addrgrp6	157
config firewall wildcard-fqdn custom	158
config firewall wildcard-fqdn group	159
config firewall service category	160
config firewall service custom	160
config firewall service group	164
config firewall city	165
config firewall region	166
config firewall country	166
config firewall internet-service	167
config firewall internet-service-name	168
config firewall internet-service-group	169
config firewall internet-service-extension	170
config firewall internet-service-reputation	172
config firewall internet-service-custom	172
config firewall internet-service-addition	174
config firewall internet-service-append	175
config firewall internet-service-custom-group	176
config firewall internet-service-sld	176
config firewall internet-service-ipbl-vendor	176
config firewall internet-service-ipbl-reason	177
config firewall internet-service-owner	177
config firewall internet-service-list	177
config firewall internet-service-definition	178
config firewall internet-service-botnet	179
config firewall vendor-mac	179
config firewall vendor-mac-summary	180
config firewall shaper traffic-shaper	180
config firewall shaper per-ip-shaper	182
config firewall shaper traffic	184
config firewall shaper per-ip	184

config firewall proxy-address	184
config firewall proxy-addrgrp	188
config firewall schedule onetime	189
config firewall schedule recurring	190
config firewall schedule group	191
config firewall ippool	192
config firewall ippool6	194
config firewall ldb-monitor	195
config firewall vip	197
config firewall vip6	228
config firewall vipgrp	257
config firewall vipgrp6	258
config firewall ssh local-key	258
config firewall ssh local-ca	259
config firewall ssh setting	260
config firewall ssh host-key	261
config firewall access-proxy-virtual-host	262
config firewall access-proxy-ssh-client-cert	263
config firewall access-proxy	265
config firewall access-proxy6	284
config firewall ipmacbinding setting	303
config firewall ipmacbinding table	304
config firewall profile-protocol-options	304
config firewall ssl-ssh-profile	328
config firewall profile-group	355
config firewall ssl-server	357
config firewall decrypted-traffic-mirror	359
config firewall identity-based-route	360
config firewall auth-portal	361
config firewall security-policy	361
config firewall policy	368
config firewall traffic-class	386
config firewall shaping-policy	386
config firewall shaping-profile	391
config firewall local-in-policy	393
config firewall local-in-policy6	395
config firewall ttl-policy	397
config firewall proxy-policy	398
config firewall dnstranslation	405
config firewall multicast-policy	406
config firewall multicast-policy6	408
config firewall interface-policy	410
config firewall interface-policy6	413
config firewall DoS-policy	416
config firewall DoS-policy6	418
config firewall sniffer	420
config firewall acl	426
config firewall acl6	427
config firewall central-snat-map	428

config firewall ssl setting	430
config firewall ip-translation	432
config firewall ipv6-eh-filter	433
config firewall iprope list	435
config firewall iprope appctrl list	435
config firewall iprope appctrl status	435
config firewall proute	435
config firewall proute6	436
ftp-proxy	437
config ftp-proxy explicit	437
hardware	439
config hardware status	439
config hardware cpu	439
config hardware memory	439
config hardware nic	439
icap	441
config icap server	441
config icap profile	442
ips	448
config ips sensor	448
config ips view-map	452
config ips decoder	453
config ips rule	454
config ips rule-settings	456
config ips custom	456
config ips global	458
config ips settings	461
config ips session	462
ipsec	463
config ipsec tunnel	463
log	464
config log threat-weight	465
config log custom-field	475
config log syslogd setting	475
config log syslogd override-setting	479
config log syslogd filter	483
config log syslogd override-filter	485
config log syslogd2 setting	488
config log syslogd2 override-setting	492
config log syslogd2 filter	496
config log syslogd2 override-filter	498
config log syslogd3 setting	501
config log syslogd3 override-setting	505
config log syslogd3 filter	508
config log syslogd3 override-filter	511
config log syslogd4 setting	514
config log syslogd4 override-setting	518
config log syslogd4 filter	521

config log syslogd4 override-filter	524
config log webtrends setting	527
config log webtrends filter	527
config log memory global-setting	530
config log memory setting	531
config log memory filter	531
config log disk setting	534
config log disk filter	539
config log eventfilter	542
config log fortiguard setting	545
config log fortiguard override-setting	547
config log fortiguard filter	549
config log fortiguard override-filter	551
config log null-device setting	554
config log null-device filter	555
config log setting	557
config log gui-display	561
config log fortianalyzer setting	562
config log fortianalyzer override-setting	566
config log fortianalyzer filter	570
config log fortianalyzer override-filter	573
config log fortianalyzer2 setting	576
config log fortianalyzer2 override-setting	580
config log fortianalyzer2 filter	584
config log fortianalyzer2 override-filter	587
config log fortianalyzer3 setting	590
config log fortianalyzer3 override-setting	594
config log fortianalyzer3 filter	598
config log fortianalyzer3 override-filter	601
config log fortianalyzer-cloud setting	604
config log fortianalyzer-cloud override-setting	607
config log fortianalyzer-cloud filter	608
config log fortianalyzer-cloud override-filter	610
mgmt-data	614
config mgmt-data status	614
router	615
config router access-list	615
config router access-list6	616
config router aspath-list	617
config router prefix-list	618
config router prefix-list6	619
config router key-chain	620
config router community-list	621
config router route-map	622
config router rip	628
config router ripng	634
config router static	639
config router policy	641
config router policy6	644

config router static6	645
config router ospf	647
config router ospf6	662
config router bgp	676
config router isis	716
config router multicast-flow	729
config router multicast	730
config router multicast6	738
config router info	740
config router info6	740
config router auth-path	740
config router setting	741
config router bfd	741
config router bfd6	742
sctp-filter	743
config sctp-filter profile	743
ssh-filter	745
config ssh-filter profile	745
switch-controller	748
config switch-controller traffic-policy	749
config switch-controller fortilink-settings	750
config switch-controller switch-interface-tag	752
config switch-controller 802-1X-settings	752
config switch-controller security-policy 802-1X	753
config switch-controller security-policy local-access	756
config switch-controller location	757
config switch-controller lldp-settings	761
config switch-controller lldp-profile	762
config switch-controller qos dot1p-map	765
config switch-controller qos ip-dscp-map	769
config switch-controller qos queue-policy	770
config switch-controller qos qos-policy	773
config switch-controller storm-control-policy	773
config switch-controller auto-config policy	775
config switch-controller auto-config default	775
config switch-controller auto-config custom	776
config switch-controller initial-config template	776
config switch-controller initial-config vlans	778
config switch-controller switch-profile	779
config switch-controller custom-command	779
config switch-controller virtual-port-pool	780
config switch-controller ptp settings	780
config switch-controller ptp policy	781
config switch-controller vlan-policy	781
config switch-controller dynamic-port-policy	782
config switch-controller managed-switch	784
config switch-controller switch-group	816
config switch-controller stp-settings	817
config switch-controller stp-instance	818

config switch-controller storm-control	818
config switch-controller global	819
config switch-controller system	823
config switch-controller switch-log	824
config switch-controller igmp-snooping	825
config switch-controller sflow	826
config switch-controller quarantine	826
config switch-controller network-monitor-settings	827
config switch-controller flow-tracking	828
config switch-controller snmp-sysinfo	830
config switch-controller snmp-trap-threshold	831
config switch-controller snmp-community	832
config switch-controller snmp-user	834
config switch-controller traffic-sniffer	836
config switch-controller remote-log	837
config switch-controller mac-policy	840
system	841
config system vdom	844
config system global	845
config system accprofile	882
config system npu	892
config system vdom-link	897
config system switch-interface	898
config system object-tagging	899
config system lte-modem	901
config system interface	902
config system physical-switch	949
config system virtual-switch	949
config system stp	951
config system password-policy	952
config system password-policy-guest-admin	954
config system sms-server	956
config system custom-language	956
config system admin	957
config system api-user	963
config system sso-admin	965
config system sso-forticloud-admin	965
config system settings	966
config system sit-tunnel	985
config system fssso-polling	986
config system ha	987
config system ha-monitor	998
config system storage	999
config system dedicated-mgmt	1000
config system arp-table	1001
config system ipv6-neighbor-cache	1002
config system dns	1002
config system ddns	1005
config system sflow	1007

config system vdom-sflow	1008
config system netflow	1009
config system vdom-netflow	1011
config system vdom-dns	1012
config system replacemsg-image	1013
config system replacemsg mail	1014
config system replacemsg http	1015
config system replacemsg webproxy	1015
config system replacemsg ftp	1016
config system replacemsg fortiguard-wf	1017
config system replacemsg spam	1018
config system replacemsg alertmail	1019
config system replacemsg admin	1019
config system replacemsg auth	1020
config system replacemsg sslvpn	1021
config system replacemsg nac-quar	1022
config system replacemsg traffic-quota	1023
config system replacemsg utm	1023
config system replacemsg icap	1024
config system replacemsg automation	1025
config system replacemsg-group	1026
config system snmp sysinfo	1037
config system snmp community	1038
config system snmp user	1045
config system autoupdate schedule	1050
config system autoupdate tunneling	1051
config system session-ttl	1052
config system dhcp server	1053
config system dhcp6 server	1064
config system modem	1068
config system 3g-modem custom	1075
config system status	1075
config system performance status	1076
config system performance top	1076
config system performance firewall packet-distribution	1076
config system performance firewall statistics	1076
config system session	1076
config system session6	1077
config system cmdb	1077
config system fortiguard-service	1077
config system fortianalyzer-connectivity	1077
config system checksum status	1077
config system mgmt-csum	1077
config system ha-nonsync-csum	1078
config system fortiguard-log-service	1078
config system central-mgmt	1078
config system alias	1078
config system auto-script	1078
config system info admin status	1079

config system info admin ssh	1080
config system management-tunnel	1080
config system fortimanager	1081
config system fm	1083
config system central-management	1084
config system zone	1088
config system geoip-country	1089
config system sdn-connector	1089
config system ipv6-tunnel	1096
config system external-resource	1097
config system ips-urlfilter-dns	1098
config system ips-urlfilter-dns6	1099
config system network-visibility	1099
config system sdwan	1101
config system gre-tunnel	1121
config system ipsec-aggregate	1123
config system ipip-tunnel	1124
config system mobile-tunnel	1125
config system pppoe-interface	1127
config system vxlan	1129
config system geneve	1130
config system virtual-wire-pair	1131
config system dns-database	1132
config system dns-server	1135
config system resource-limits	1136
config system vdom-property	1139
config system speed-test-server	1141
config system lldp network-policy	1142
config system speed-test-schedule	1149
config system standalone-cluster	1151
config system cluster-sync	1152
config system fortiguard	1155
config system ips	1162
config system arp	1163
config system email-server	1163
config system alarm	1165
config system mac-address-table	1168
config system session-helper	1169
config system proxy-arp	1170
config system fips-cc	1170
config system tos-based-priority	1171
config system dscp-based-priority	1172
config system probe-response	1173
config system link-monitor	1174
config system auto-install	1179
config system console	1179
config system ntp	1181
config system ptp	1183
config system wccp	1185

config system dns64	1188
config system vdom-radius-server	1189
config system startup-error-log	1190
config system source-ip status	1190
config system auto-update status	1190
config system auto-update versions	1190
config system session-info list	1190
config system session-info expectation	1191
config system session-info full-stat	1191
config system session-info statistics	1191
config system session-info ttl	1191
config system session-helper-info list	1191
config system ip-conflict status	1191
config system ftm-push	1192
config system geoip-override	1192
config system fortisandbox	1193
config system fortiai	1195
config system vdom-exception	1196
config system csf	1197
config system automation-trigger	1201
config system automation-action	1205
config system automation-destination	1210
config system automation-stitch	1210
config system nd-proxy	1211
config system saml	1212
config system federated-upgrade	1215
config system vne-tunnel	1217
config system ike	1218
config system acme	1232
test	1233
config test smtp	1234
config test ftpd	1235
config test pop3	1235
config test imap	1235
config test nntp	1236
config test harelay	1236
config test hasync	1236
config test hatalk	1237
config test sessionsync	1237
config test forticldd	1237
config test miglogd	1238
config test syslogd	1238
config test urlfilter	1238
config test wf_monitor	1239
config test ovrd	1239
config test iotd	1239
config test ipsmonitor	1240
config test ipsengine	1240
config test ipldbd	1240

config test ddnsd	1241
config test snmpd	1241
config test acd	1241
config test dnsproxy	1242
config test sflood	1242
config test init	1242
config test l2tpcd	1243
config test dhcprelay	1243
config test pptpcd	1243
config test wccpd	1244
config test wad	1244
config test radiusd	1244
config test fsd	1245
config test ipsufd	1245
config test lted	1245
config test forticron	1246
config test uploadd	1246
config test quarantined	1246
config test dhcp6c	1247
config test dsd	1247
config test ipmc_sensord	1247
config test lnkmtd	1248
config test dhcp6r	1248
config test updated	1248
config test awsd	1249
config test netxd	1249
config test fnbamd	1249
config test mrd	1250
config test zebos_launcher	1250
config test radius-das	1250
config test wiredapd	1251
config test csfd	1251
config test fsvrd	1251
config test radvd	1252
config test fcnacd	1252
config test sdncd	1252
config test azd	1253
config test gcpd	1253
config test ocid	1253
config test kubed	1254
config test autod	1254
config test bfd	1254
config test openstackd	1255
config test fas	1255
config test sepmd	1255
config test ipamd	1256
config test sdnd	1256
config test vned	1256
config test sfupgraded	1257

config test fds_notify	1257
user	1258
config user certificate	1258
config user radius	1259
config user tacacs+	1270
config user exchange	1272
config user ldap	1274
config user krb-keytab	1280
config user domain-controller	1281
config user pop3	1284
config user saml	1285
config user fssso	1289
config user adgrp	1292
config user fssso-polling	1293
config user fortitoken	1295
config user password-policy	1295
config user local	1296
config user setting	1299
config user peer	1303
config user peergrp	1305
config user quarantine	1305
config user group	1307
config user security-exempt-list	1312
config user hac-policy	1312
videofilter	1315
config videofilter youtube-key	1315
config videofilter youtube-channel-filter	1315
config videofilter profile	1316
voip	1319
config voip profile	1319
vpn	1343
config vpn certificate ca	1344
config vpn certificate remote	1345
config vpn certificate local	1346
config vpn certificate crl	1349
config vpn certificate ocsp-server	1351
config vpn certificate setting	1351
config vpn ssl web realm	1356
config vpn ssl web host-check-software	1357
config vpn ssl web portal	1359
config vpn ssl web user-group-bookmark	1376
config vpn ssl web user-bookmark	1382
config vpn ssl settings	1388
config vpn ssl client	1401
config vpn ssl monitor	1402
config vpn ipsec phase1	1402
config vpn ipsec phase2	1421
config vpn ipsec manualkey	1430
config vpn ipsec concentrator	1432

config vpn ipsec phase1-interface	1432
config vpn ipsec phase2-interface	1456
config vpn ipsec manualkey-interface	1465
config vpn ipsec forticlient	1467
config vpn ipsec stats crypto	1468
config vpn ipsec stats tunnel	1468
config vpn ipsec tunnel details	1468
config vpn ipsec tunnel summary	1468
config vpn ipsec tunnel name	1469
config vpn pptp	1469
config vpn l2tp	1470
config vpn ovpn	1471
config vpn ike gateway	1475
config vpn status l2tp	1475
config vpn status pptp	1475
config vpn status ssl list	1476
config vpn status ssl hw-acceleration-status	1476
waf	1477
config waf main-class	1477
config waf sub-class	1477
config waf signature	1478
config waf profile	1478
web-proxy	1503
config web-proxy profile	1503
config web-proxy global	1507
config web-proxy explicit	1509
config web-proxy forward-server	1514
config web-proxy forward-server-group	1516
config web-proxy debug-url	1517
config web-proxy wisp	1518
config web-proxy url-match	1519
webfilter	1521
config webfilter ftgd-local-cat	1521
config webfilter content	1522
config webfilter content-header	1523
config webfilter urlfilter	1524
config webfilter ips-urlfilter-setting	1527
config webfilter ips-urlfilter-setting6	1528
config webfilter ips-urlfilter-cache-setting	1528
config webfilter profile	1529
config webfilter fortiguard	1545
config webfilter categories	1547
config webfilter override	1547
config webfilter ftgd-local-rating	1549
config webfilter search-engine	1549
config webfilter ftgd-statistics	1550
config webfilter status	1550
config webfilter override-usr	1551
wireless-controller	1552

config wireless-controller inter-controller	1553
config wireless-controller global	1554
config wireless-controller hotspot20 anqp-venue-name	1557
config wireless-controller hotspot20 anqp-network-auth-type	1558
config wireless-controller hotspot20 anqp-roaming-consortium	1559
config wireless-controller hotspot20 anqp-nai-realm	1559
config wireless-controller hotspot20 anqp-3gpp-cellular	1562
config wireless-controller hotspot20 anqp-ip-address-type	1563
config wireless-controller hotspot20 h2qp-operator-name	1564
config wireless-controller hotspot20 h2qp-wan-metric	1564
config wireless-controller hotspot20 h2qp-conn-capability	1566
config wireless-controller hotspot20 icon	1568
config wireless-controller hotspot20 h2qp-osu-provider	1569
config wireless-controller hotspot20 qos-map	1571
config wireless-controller hotspot20 hs-profile	1572
config wireless-controller vap	1579
config wireless-controller timers	1607
config wireless-controller setting	1609
config wireless-controller log	1618
config wireless-controller apcfg-profile	1623
config wireless-controller bonjour-profile	1624
config wireless-controller arrp-profile	1625
config wireless-controller region	1628
config wireless-controller vap-group	1629
config wireless-controller wids-profile	1629
config wireless-controller ble-profile	1636
config wireless-controller wtp-profile	1638
config wireless-controller wtp	1707
config wireless-controller wtp-group	1729
config wireless-controller qos-profile	1732
config wireless-controller wag-profile	1735
config wireless-controller utm-profile	1737
config wireless-controller address	1738
config wireless-controller addgrp	1738
config wireless-controller snmp	1739
config wireless-controller mpsk-profile	1742
config wireless-controller nac-profile	1744
config wireless-controller ssid-policy	1745
config wireless-controller access-control-list	1745
config wireless-controller scan	1747
config wireless-controller ap-status	1747
config wireless-controller wlchanlistlic	1748
config wireless-controller status	1748
config wireless-controller wtp-status	1749
config wireless-controller client-info	1749
config wireless-controller vap-status	1749
config wireless-controller rf-analysis	1750
config wireless-controller spectral-info	1750

Change Log

Date	Change Description
2021-07-16	First automated release of the FortiOS 7.0.1 CLI Reference.
2021-07-20	<p>Updated config user fss0 on page 1289 to add the collector agent maximum password length.</p> <p>Updated config system global on page 845 to add additional information for dnsproxy-worker-count and cloud-communication.</p> <p>Updated config system resource-limits on page 1136 to add additional information for log-disk-quota .</p>

FortiOS CLI reference

This document describes FortiOS 7.0.1 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI). For information on using the CLI, see the [FortiOS 7.0.1 Administration Guide](#), which contains information such as:

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

If you have comments on this content, its format, or requests for commands that are not included, contact us at techdoc@fortinet.com.

Creation of the CLI reference

The CLI syntax is created by processing the schema from FortiGate models running FortiOS 7.0.1 and reformatting the resultant CLI output. The following reference models were used to create this CLI reference:

- *FGT_140E_POE*: a POE model with 40 x GE RJ45 (including 24 x RJ45 GE POE/POE+ ports, 14 x switch ports, 1 x MGMT port, 1x HA port, 2 x WAN ports), 2 x GE SFP DMZ slots.
- *FWF_61F*: a WiFi/desktop model with 10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2), 128GB SSD onboard storage.
- *FGT_501E*: a mid-range model with 2x 240GB SSD storage, NP6 and CP9 acceleration, 2x 10GE SFP+ slots, 8x GE SFP slots and 10x GE RJ45 ports.
- *FGT_3000D*: a high-end model with 480GB SSD storage, NP6 and CP8 acceleration, dyak AC power supplies, 16x 10GE SFP+ slots and 2x GE RJ45 management ports.
- *FGT_VM64*: a Virtual Machine model running on VMware ESXi.

Availability of commands and options

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

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

FortiGate model

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

Hardware configuration

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

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

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

CLI configuration commands

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



The command branches are in alphabetical order. The commands beneath each branch are *not* in alphabetical order.

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 21](#)

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 sslvpn-authentication-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 FDS-license-expiring-days {integer}
  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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>category</i></td><td>Filter based on category.</td></tr> <tr> <td><i>threshold</i></td><td>Filter based on severity.</td></tr> </tbody> </table>					Option	Description	<i>category</i>	Filter based on category.	<i>threshold</i>	Filter based on severity.
Option	Description									
<i>category</i>	Filter based on category.									
<i>threshold</i>	Filter based on severity.									
email-interval	Interval between sending alert emails .	integer	Minimum value: 1 Maximum value: 99999	5						
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable IPS logs in alert email.</td></tr> <tr> <td><i>disable</i></td><td>Disable IPS logs in alert email.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable IPS logs in alert email.	<i>disable</i>	Disable IPS logs in alert email.
Option	Description									
<i>enable</i>	Enable IPS logs in alert email.									
<i>disable</i>	Disable IPS logs in alert email.									
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable firewall authentication failure logs in alert email.</td></tr> <tr> <td><i>disable</i></td><td>Disable firewall authentication failure logs in alert email.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable firewall authentication failure logs in alert email.	<i>disable</i>	Disable firewall authentication failure logs in alert email.
Option	Description									
<i>enable</i>	Enable firewall authentication failure logs in alert email.									
<i>disable</i>	Disable firewall authentication failure logs in alert email.									
HA-logs	Enable/disable HA logs in alert email.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.									

Parameter	Description	Type	Size	Default
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPsec error logs in alert email.		
	<i>disable</i>	Disable IPsec error logs in alert email.		
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-	disable
	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
	Option	Description		
	<i>enable</i>	Enable PPP error logs in alert email.		
	<i>disable</i>	Disable PPP error logs in alert email.		
sslvpn-authentication-errors-logs	Enable/disable SSL-VPN authentication error logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.		
	<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.		
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-	disable
	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
	Option	Description		
	<i>enable</i>	Enable web filter logs in alert email.		
	<i>disable</i>	Disable web filter logs in alert email.		
configuration-changes-logs	Enable/disable configuration change logs in alert email.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable configuration change logs in alert email.		
	disable	Disable configuration change logs in alert email.		
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-	disable
	Option	Description		
	enable	Enable violation traffic logs in alert email.		
	disable	Disable violation traffic logs in alert email.		
admin-login-logs	Enable/disable administrator login/logout logs in alert email.	option	-	disable
	Option	Description		
	enable	Enable administrator login/logout logs in alert email.		
	disable	Disable administrator login/logout logs in alert email.		
FDS-license-expiring-warning	Enable/disable FortiGuard license expiration warnings in alert email.	option	-	disable
	Option	Description		
	enable	Enable FortiGuard license expiration warnings in alert email.		
	disable	Disable FortiGuard license expiration warnings in alert email.		
log-disk-usage-warning	Enable/disable disk usage warnings in alert email.	option	-	disable
	Option	Description		
	enable	Enable disk usage warnings in alert email.		
	disable	Disable disk usage warnings in alert email.		
fortiguard-log-quota-warning	Enable/disable FortiCloud log quota warnings in alert email.	option	-	disable
	Option	Description		
	enable	Enable FortiCloud log quota warnings in alert email.		
	disable	Disable FortiCloud log quota warnings in alert email.		
amc-interface-bypass-mode	Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		
	disable	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
	Option	Description		
	enable	Enable FIPS and Common Criteria error logs in alert email.		
	disable	Disable FIPS and Common Criteria error logs in alert email.		
FSSO-disconnect-logs	Enable/disable logging of FSSO collector agent disconnect.	option	-	disable
	Option	Description		
	enable	Enable logging of FSSO collector agent disconnect.		
	disable	Disable logging of FSSO collector agent disconnect.		
ssh-logs	Enable/disable SSH logs in alert email.	option	-	disable
	Option	Description		
	enable	Enable SSH logs in alert email.		
	disable	Disable SSH logs in alert email.		
FDS-license-expiring-days	Number of days to send alert email prior to FortiGuard license expiration .	integer	Minimum value: 1 Maximum value: 100	15
local-disk-usage	Disk usage percentage at which to send alert email .	integer	Minimum value: 1 Maximum value: 99	75
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	1

Parameter	Description	Type	Size	Default
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
Option	Description			
<i>emergency</i>	Emergency level.			
<i>alert</i>	Alert level.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		

antivirus

This section includes syntax for the following commands:

- [config antivirus profile on page 34](#)
- [config antivirus quarantine on page 29](#)
- [config antivirus settings on page 28](#)

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}
end
```

config antivirus settings

Parameter	Description	Type	Size	Default
machine-learning-detection	Use machine learning based malware detection.	option	-	enable
Option	Description			
<i>enable</i>	Enable machine learning based malware detection.			
<i>monitor</i>	Enable machine learning based malware detection for monitoring only.			
<i>disable</i>	Disable machine learning based malware detection.			
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable
Option	Description			
<i>enable</i>	Enable extreme AVDB.			
<i>disable</i>	Disable extreme AVDB.			
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	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 . 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

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-blocked {option1}, {option2}, ...
  set store-blocked {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 .	integer	Minimum value: 0 Maximum value: 479	0
maxfilesize	Maximum file size to quarantine .	integer	Minimum value: 0 Maximum value: 500	0
quarantine-quota	The amount of disk space to reserve for quarantining files .	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
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		
	<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>smt�</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 smt� pop3s https ft� mapi cifs ssh
	Option	Description		
	<i>imap</i>	IMAP.		
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>http</i>	HTTP.		
	<i>ftp</i>	FTP.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>nntp</i>	NNTP.		
	<i>imaps</i>	IMAPS.		
	<i>smt�</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.		
drop-blocked	Do not quarantine dropped files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-	
	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>smt�</i>	SMTPS.		
	<i>pop3s</i>	POP3S.		
	<i>ftps</i>	FTPS.		
	<i>mapi</i>	MAPI.		
	<i>cifs</i>	CIFS.		
	<i>ssh</i>	SSH.		

Parameter	Description	Type	Size	Default
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtpls pop3s ftps mapi cifs ssh
Option				
<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>smtpls</i>	SMTPLS.			
<i>pop3s</i>	POP3S.			
<i>ftpls</i>	FTPLS.			
<i>mapi</i>	MAPI.			
<i>cifs</i>	CIFS.			
<i>ssh</i>	SSH.			
drop-machine-learning	Do not quarantine files detected by machine learning found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-	
Option				
<i>imap</i>	IMAP.			
<i>smtp</i>	SMTP.			
<i>pop3</i>	POP3.			
<i>http</i>	HTTP.			
<i>ftp</i>	FTP.			
<i>nntp</i>	NNTP.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>imaps</i>	IMAPS.		
	<i>smt�</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-machine-learning	Quarantine files detected by machine learning found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smt� pop3s https ft� mapi cifs ssh
	Option	Description		
	<i>imap</i>	IMAP.		
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>http</i>	HTTP.		
	<i>ftp</i>	FTP.		
	<i>nntp</i>	NNTP.		
	<i>imaps</i>	IMAPS.		
	<i>smt�</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
lowspace	Select the method for handling additional files when running low on disk space.	option	-	ovrw-old
	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 FortiGate disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	NULL **
	Option	Description		
	<i>NULL</i>	Files that would be quarantined are deleted.		
	<i>disk</i>	Quarantine files to the FortiGate hard disk.		
	<i>FortiAnalyzer</i>	FortiAnalyzer		

** Values may differ between models.

config antivirus profile

Configure AntiVirus profiles.

```
config antivirus profile
  Description: Configure AntiVirus profiles.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set feature-set [flow|proxy]
    set ftgd-analytics [disable|suspicious|...]
    set analytics-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 fortiai [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 fortiai [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 fortiai [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 fortiai [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 fortiai [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 fortiai [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 fortiai [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 fortiai [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 fortiai [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 fortiai-error-action [log-only|block|...]
    set av-virus-log [enable|disable]
    set av-block-log [enable|disable]
    set extended-log [enable|disable]
    set scan-mode [default|legacy]
next
end

```

config antivirus profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35	
feature-set	Flow/proxy feature set.	option	-	flow
Option		Description		
		<i>flow</i> Flow feature set.		
		<i>proxy</i> Proxy feature set.		
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-	disable
Option		Description		
		<i>disable</i> Do not upload files to FortiSandbox.		
		<i>suspicious</i> Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.		
		<i>everything</i> Submit all files scanned by AntiVirus to FortiSandbox. AntiVirus may not scan all files.		

Parameter	Description	Type	Size	Default						
analytics-max-upload	Maximum size of files that can be uploaded to FortiSandbox.	integer	Minimum value: 1 Maximum value: 383 **	10						
analytics-ignore-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0						
analytics-accept-filetype	Only submit files matching this DLP file-pattern to FortiSandbox.	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Use only the standard AV signature databases.</td></tr> <tr> <td><i>enable</i></td><td>Also use the FortiSandbox signature database.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Use only the standard AV signature databases.	<i>enable</i>	Also use the FortiSandbox signature database.
Option	Description									
<i>disable</i>	Use only the standard AV signature databases.									
<i>enable</i>	Also use the FortiSandbox signature database.									
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Do not use the mobile malware signature database.</td></tr> <tr> <td><i>enable</i></td><td>Also use the mobile malware signature database.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Do not use the mobile malware signature database.	<i>enable</i>	Also use the mobile malware signature database.
Option	Description									
<i>disable</i>	Do not use the mobile malware signature database.									
<i>enable</i>	Also use the mobile malware signature database.									
outbreak-prevention-archive-scan	Enable/disable outbreak-prevention archive scanning.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Analyze files as sent, not the content of archives.</td></tr> <tr> <td><i>enable</i></td><td>Analyze files including the content of archives.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Analyze files as sent, not the content of archives.	<i>enable</i>	Analyze files including the content of archives.
Option	Description									
<i>disable</i>	Analyze files as sent, not the content of archives.									
<i>enable</i>	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.		
fortiai-error-action	Action to take if FortiAI encounters an error.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Log FortiAI error, but allow the file.		
	<i>block</i>	Block the file on FortiAI error.		
	<i>ignore</i>	Do nothing on FortiAI error.		
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
extended-log	Enable/disable extended logging for antivirus.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
scan-mode	Choose between default scan mode and legacy scan mode.	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.		

** Values may differ between models.

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.		
	<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.		
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		

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

Parameter	Description	Type	Size	Default
emulator	Enable/disable the virus emulator.	option	-	enable
	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
	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.		

Parameter	Description	Type	Size	Default
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiAI detected infections.		
	<i>monitor</i>	Log the FortiAI 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>fileslimit</i>	Block exceeded archive files limit.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>filelimit</i>	Log exceeded archive files limit.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS 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 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.		
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS 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.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option	Description		
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	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.		

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.																	
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																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.																							
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>block</i></td><td>Block the FortiAI detected infections.</td></tr> <tr> <td><i>monitor</i></td><td>Log the FortiAI detected infections.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiAI detected infections.	<i>monitor</i>	Log the FortiAI detected infections.															
Option	Description																							
<i>disable</i>	Disable.																							
<i>block</i>	Block the FortiAI detected infections.																							
<i>monitor</i>	Log the FortiAI detected infections.																							
quarantine	Enable/disable quarantine for infected files.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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>fileslimit</i></td><td>Block exceeded archive files limit.</td></tr> <tr> <td><i>timeout</i></td><td>Block scan timeout.</td></tr> <tr> <td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr> </tbody> </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>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							

Parameter	Description	Type	Size	Default																				
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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>fileslimit</i></td><td>Log exceeded archive files limit.</td></tr> <tr> <td><i>timeout</i></td><td>Log scan timeout.</td></tr> <tr> <td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr> </tbody> </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>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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

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.		
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiAI detected infections.		
	<i>monitor</i>	Log the FortiAI 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.		

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

Parameter	Description	Type	Size	Default
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
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 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
Option	Description			
<i>disable</i>	Disable.			
<i>block</i>	Block the matched files.			
<i>monitor</i>	Log the matched files.			
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable
Option	Description			
<i>disable</i>	Disable.			
<i>block</i>	Block the FortiAI detected infections.			
<i>monitor</i>	Log the FortiAI detected infections.			

Parameter	Description	Type	Size	Default																				
quarantine	Enable/disable quarantine for infected files.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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>fileslimit</i></td><td>Block exceeded archive files limit.</td></tr> <tr> <td><i>timeout</i></td><td>Block scan timeout.</td></tr> <tr> <td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr> </tbody> </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>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.
Option	Description																							
<i>encrypted</i>	Block encrypted archives.																							
<i>corrupted</i>	Block corrupted archives.																							
<i>partiallycorrupted</i>	Block partially corrupted archives.																							
<i>multipart</i>	Block multipart archives.																							
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																							
<i>mailbomb</i>	Block mail bomb archives.																							
<i>fileslimit</i>	Block exceeded archive files limit.																							
<i>timeout</i>	Block scan timeout.																							
<i>unhandled</i>	Block archives that FortiOS cannot open.																							
archive-log	Select the archive types to log.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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>fileslimit</i></td><td>Log exceeded archive files limit.</td></tr> <tr> <td><i>timeout</i></td><td>Log scan timeout.</td></tr> <tr> <td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr> </tbody> </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>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.
Option	Description																							
<i>encrypted</i>	Log encrypted archives.																							
<i>corrupted</i>	Log corrupted archives.																							
<i>partiallycorrupted</i>	Log partially corrupted archives.																							
<i>multipart</i>	Log multipart archives.																							
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																							
<i>mailbomb</i>	Log mail bomb archives.																							
<i>fileslimit</i>	Log exceeded archive files limit.																							
<i>timeout</i>	Log scan timeout.																							
<i>unhandled</i>	Log archives that FortiOS cannot open.																							
emulator	Enable/disable the virus emulator.	option	-	enable																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option	Description		
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		

config nntp

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.		
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS 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 cifs

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.		
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS 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
	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.		
fortiai	Enable/disable scanning of files by FortiAI server.	option	-	disable

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS 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 nac-quar

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

config content-disarm

Parameter	Description	Type	Size	Default
original-file-destination	Destination to send original file if active content is removed.	option	-	discard
	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.		

Parameter	Description	Type	Size	Default
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only
	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
	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

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-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.		
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-	enable
	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
	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

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.			

application

This section includes syntax for the following commands:

- [config application list on page 67](#)
- [config application name on page 64](#)
- [config application group on page 75](#)
- [config application custom on page 66](#)
- [config application rule-settings on page 67](#)

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
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
default value	Parameter default value.	string	Maximum length: 199	

config metadata

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

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
id	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	string	Maximum length: 63	
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095	

Parameter	Description	Type	Size	Default
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 rule-settings

Configure application rule settings.

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

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 shaper-reverse {string}
    set per-ip-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
comment	comments	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
extended-log	Enable/disable extended logging.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
other-application-action	Action for other applications.	option	-	pass						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>pass</i></td><td>Allow sessions matching an application in this application list.</td></tr> <tr> <td><i>block</i></td><td>Block sessions matching an application in this application list.</td></tr> </tbody> </table>	Option	Description	<i>pass</i>	Allow sessions matching an application in this application list.	<i>block</i>	Block sessions matching an application in this application list.			
Option	Description									
<i>pass</i>	Allow sessions matching an application in this application list.									
<i>block</i>	Block sessions matching an application in this application list.									
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable replacement messages for blocked applications.</td></tr> <tr> <td><i>enable</i></td><td>Enable replacement messages for blocked applications.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable replacement messages for blocked applications.	<i>enable</i>	Enable replacement messages for blocked applications.			
Option	Description									
<i>disable</i>	Disable replacement messages for blocked applications.									
<i>enable</i>	Enable replacement messages for blocked applications.									
other-application-log	Enable/disable logging for other applications.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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						

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>pass</i>	Pass or allow unknown applications.		
	<i>block</i>	Drop or block unknown applications.		
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging for unknown applications.		
	<i>enable</i>	Enable logging for unknown applications.		
p2p-block-list	P2P applications to be blocklisted.	option	-	
	Option	Description		
	<i>skype</i>	Skype.		
	<i>edonkey</i>	Edonkey.		
	<i>bittorrent</i>	Bit torrent.		
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable deep application inspection.		
	<i>enable</i>	Enable deep application inspection.		
options	Basic application protocol signatures allowed by default.	option	-	allow-dns
	Option	Description		
	<i>allow-dns</i>	Allow DNS.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow-icmp</i>	Allow ICMP.		
	<i>allow-http</i>	Allow generic HTTP web browsing.		
	<i>allow-ssl</i>	Allow generic SSL communication.		
	<i>allow-quic</i>	Allow QUIC.		
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable protocol enforcement over selected ports.		
	<i>enable</i>	Enable protocol enforcement over selected ports.		

config entries

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

Parameter	Description	Type	Size	Default												
popularity	Application popularity filter .	option	-	1 2 3 4 5												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> <tr> <td><i>reset</i></td><td>Reset sessions for matching traffic.</td></tr> </tbody> </table>	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.							
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												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable logging.</td></tr> <tr> <td><i>enable</i></td><td>Enable logging.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable packet logging.</td></tr> <tr> <td><i>enable</i></td><td>Enable packet logging.</td></tr> </tbody> </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.															
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0												

Parameter	Description	Type	Size	Default												
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60												
rate-mode	Rate limit mode.	option	-	continuous												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>periodical</i></td><td>Allow configured number of packets every rate-duration.</td></tr> <tr> <td><i>continuous</i></td><td>Block packets once the rate is reached.</td></tr> </tbody> </table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.									
Option	Description															
<i>periodical</i>	Allow configured number of packets every rate-duration.															
<i>continuous</i>	Block packets once the rate is reached.															
rate-track	Track the packet protocol field.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>none</td></tr> <tr> <td><i>src-ip</i></td><td>Source IP.</td></tr> <tr> <td><i>dest-ip</i></td><td>Destination IP.</td></tr> <tr> <td><i>dhcp-client-mac</i></td><td>DHCP client.</td></tr> <tr> <td><i>dns-domain</i></td><td>DNS domain.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
Option	Description															
<i>none</i>	none															
<i>src-ip</i>	Source IP.															
<i>dest-ip</i>	Destination IP.															
<i>dhcp-client-mac</i>	DHCP client.															
<i>dns-domain</i>	DNS domain.															
session-ttl	Session TTL .	integer	Minimum value: 0 Maximum value: 4294967295	0												
shaper	Traffic shaper.	string	Maximum length: 35													
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35													
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35													
quarantine	Quarantine method.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>Quarantine is disabled.</td></tr> <tr> <td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
Option	Description															
<i>none</i>	Quarantine is disabled.															
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.															
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified	5m												

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

config members

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

config default-network-services

Parameter	Description	Type	Size	Default
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0
services	Network protocols.	option	-	
Parameter	Description	Type	Size	Default
Option	Description			
<i>http</i>	HTTP.			
<i>ssh</i>	SSH.			
<i>telnet</i>	TELNET.			
<i>ftp</i>	FTP.			
<i>dns</i>	DNS.			
<i>smtp</i>	SMTP.			
<i>pop3</i>	POP3.			
<i>imap</i>	IMAP.			
<i>snmp</i>	SNMP.			
<i>nntp</i>	NNTP.			
<i>https</i>	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 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
comment	Comment	var-string	Maximum length: 255	
type	Application group type.	option	-	application
	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	

Parameter	Description	Type	Size	Default
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 .	option	-	1 2 3 4 5
Option	Description			
1	Popularity level 1.			
2	Popularity level 2.			
3	Popularity level 3.			
4	Popularity level 4.			
5	Popularity level 5.			

authentication

This section includes syntax for the following commands:

- [config authentication scheme on page 77](#)
- [config authentication rule on page 79](#)
- [config authentication setting on page 81](#)

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 fssso-agent-for-ntlm {string}
    set require-tfa [enable|disable]
    set fssso-guest [enable|disable]
    set user-cert [enable|disable]
    set user-database <name1>, <name2>, ...
    set ssh-ca {string}
  next
end
```

config authentication scheme

Parameter	Description	Type	Size	Default
method	Authentication methods .	option	-	
	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>fssso</i>	Fortinet Single Sign-On (FSSO) authentication.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
negotiate-ntlm	Enable/disable negotiate authentication for NTLM .	option	-	enable
	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	
saml-timeout	SAML authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120
fssouseragent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35	
require-tfa	Enable/disable two-factor authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable two-factor authentication.		
	<i>disable</i>	Disable two-factor authentication.		
fssouserguest	Enable/disable user fssouserguest authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable user fssouserguest authentication.		
	<i>disable</i>	Disable user fssouserguest authentication.		
user-cert	Enable/disable authentication with user certificate .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable client certificate field authentication.		
	<i>disable</i>	Disable client certificate field authentication.		
user-database <name>	Authentication server to contain user information; "local" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79	
ssh-ca	SSH CA name.	string	Maximum length: 35	

config authentication rule

Configure Authentication Rules.

```
config authentication rule
  Description: Configure Authentication Rules.
  edit <name>
    set status [enable|disable]
    set protocol [http|ftp|...]
    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 transaction-based [enable|disable]
    set web-portal [enable|disable]
    set comments {var-string}
  next
end
```

config authentication rule

Parameter	Description	Type	Size	Default
status	Enable/disable this authentication rule.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this authentication rule.		
	<i>disable</i>	Disable this authentication rule.		
protocol	Authentication is required for the selected protocol .	option	-	http

Parameter	Description	Type	Size	Default
	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.		
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
	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 .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Web authentication cookie.		
	<i>disable</i>	Disable Web authentication cookie.		

Parameter	Description	Type	Size	Default
transaction-based	Enable/disable transaction based authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable transaction based authentication.		
	<i>disable</i>	Disable transaction based authentication.		
web-portal	Enable/disable web portal for proxy transparent policy .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable web-portal.		
	<i>disable</i>	Disable web-portal.		
comments	Comment.	var-string	Maximum length: 1023	

config authentication setting

Configure authentication setting.

```
config authentication setting
  Description: Configure authentication setting.
  set active-auth-scheme {string}
  set sso-auth-scheme {string}
  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>, ...
end
```

config authentication setting

Parameter	Description	Type	Size	Default
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35	
captive-portal-type	Captive portal type.	option	-	fqdn
	Option	Description		
	<i>fqdn</i>	Use FQDN for captive portal.		
	<i>ip</i>	Use an IP address for captive portal.		
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
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	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 .	integer	Minimum value: 1 Maximum value: 65535	7832
captive-portal-port	Captive portal port number .	integer	Minimum value: 1 Maximum value: 65535	7830

Parameter	Description	Type	Size	Default
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
captive-portal-ssl-port	Captive portal SSL port number .	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	

certificate

This section includes syntax for the following commands:

- [config certificate ca on page 84](#)
- [config certificate local on page 86](#)
- [config certificate remote on page 85](#)
- [config certificate crl on page 89](#)

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 auto-update-days {integer}
    set auto-update-days-warning {integer}
    set source-ip {ipv4-address}
  next
end
```

config certificate ca

Parameter	Description	Type	Size	Default
ca	CA certificate as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the CA certificate.	option	-	global
Option		Description		
		<i>global</i> Global range.		
		<i>vdom</i> VDOM IP address range.		
source	CA certificate source type.	option	-	user
Option		Description		
		<i>factory</i> Factory installed certificate.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
	Option	Description		
	<i>enable</i>	Trusted CA for SSL inspection.		
	<i>disable</i>	Untrusted CA for SSL inspection.		
scep-url	URL of the SCEP server.	string	Maximum length: 255	
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated .	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

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
remote	Remote certificate.	user	Not Specified	
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.		

config certificate local

Local keys and certificates.

```
config certificate local
  Description: Local keys and certificates.
  edit <name>
    set password {password}
    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 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}
next
end

```

config certificate local

Parameter	Description	Type	Size	Default								
password	Password as a PEM file.	password	Not Specified									
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									
range	Either a global or VDOM IP address range for the certificate.	option	-	global								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>global</i></td><td>Global range.</td></tr> <tr> <td><i>vdom</i></td><td>VDOM IP address range.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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								

Parameter	Description	Type	Size	Default										
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0										
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>printable</i></td><td>Printable encoding (default).</td></tr> <tr> <td><i>utf8</i></td><td>UTF-8 encoding.</td></tr> </tbody> </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 FortiGate uses for authentication as a VPN client.	string	Maximum length: 63											
ike-localid-type	IKE local ID type.	option	-	asn1dn										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.
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.													
cmp-server	'ADDRESS:PORT' for CMP server.	string	Maximum length: 63											

Parameter	Description	Type	Size	Default
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	-	keyupdate
	Option	Description		
	<i>keyupdate</i>	Key Update.		
	<i>renewal</i>	Renewal.		
acme-ca-url	The URL for the ACME CA server .	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this Fortigate.	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 .	integer	Minimum value: 1 Maximum value: 60	30

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
crl	Certificate Revocation List as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the certificate.	option	-	global
	Option	Description		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
source	Certificate source type.	option	-	user
	Option	Description		
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
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

Parameter	Description	Type	Size	Default
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0

dlp

This section includes syntax for the following commands:

- [config dlp sensitivity on page 95](#)
- [config dlp sensor on page 95](#)
- [config dlp filepattern on page 92](#)

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
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.	

Parameter	Description	Type	Size	Default
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>hta</i>	Match hta files.			
<i>html</i>	Match html files.			
<i>jad</i>	Match jad files.			
<i>class</i>	Match class files.			
<i>cod</i>	Match cod files.			
<i>javascript</i>	Match javascript files.			
<i>msoffice</i>	Match 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.			

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

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 sensor

Configure DLP sensors.

```
config dlp sensor
    Description: Configure DLP sensors.
    edit <name>
        set comment {var-string}
        set feature-set [flow|proxy]
        set replacemsg-group {string}
        config filter
            Description: Set up DLP filters for this sensor.
            edit <id>
                set name {string}
                set severity [info|low|...]
                set type [file|message]
                set proto {option1}, {option2}, ...
                set filter-by [credit-card|ssn|...]
                set file-size {integer}
                set company-identifier {string}
                set sensitivity <name1>, <name2>, ...
                set file-type {integer}
                set regexp {string}
                set archive [disable|enable]
                set action [allow|log-only|...]
                set expiry {user}
            next
        end
        set dlp-log [enable|disable]
        set extended-log [enable|disable]
        set nac-quar-log [enable|disable]
        set full-archiveproto {option1}, {option2}, ...
        set summaryproto {option1}, {option2}, ...
    next
end
```

config dlp sensor

Parameter	Description	Type	Size	Default										
comment	Comment.	var-string	Maximum length: 255											
feature-set	Flow/proxy feature set.	option	-	flow										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>flow</i></td><td>Flow feature set.</td></tr> <tr> <td><i>proxy</i></td><td>Proxy feature set.</td></tr> </tbody> </table>	Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.							
Option	Description													
<i>flow</i>	Flow feature set.													
<i>proxy</i>	Proxy feature set.													
replacemsg-group	Replacement message group used by this DLP sensor.	string	Maximum length: 35											
dlp-log	Enable/disable DLP logging.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable DLP logging.</td></tr> <tr> <td><i>disable</i></td><td>Disable DLP logging.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP logging.	<i>disable</i>	Disable DLP logging.							
Option	Description													
<i>enable</i>	Enable DLP logging.													
<i>disable</i>	Disable DLP logging.													
extended-log	Enable/disable extended logging for data leak prevention.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
nac-quar-log	Enable/disable NAC quarantine logging.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable NAC quarantine logging.</td></tr> <tr> <td><i>disable</i></td><td>Disable NAC quarantine logging.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable NAC quarantine logging.	<i>disable</i>	Disable NAC quarantine logging.							
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	-											
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.			
Option	Description													
<i>smtp</i>	SMTP.													
<i>pop3</i>	POP3.													
<i>imap</i>	IMAP.													
<i>http-get</i>	HTTP GET.													

Parameter	Description	Type	Size	Default
	Option	Description		
	<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	-	
	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 filter

Parameter	Description	Type	Size	Default
name	Filter name.	string	Maximum length: 35	
severity	Select the severity or threat level that matches this filter.	option	-	medium
	Option	Description		
	<i>info</i>	Informational.		
	<i>low</i>	Low.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>medium</i>	Medium.		
	<i>high</i>	High.		
	<i>critical</i>	Critical.		
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file
	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	Select messages or files over one or more of these protocols.	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.		
filter-by	Select the type of content to match.	option	-	credit-card
	Option	Description		
	<i>credit-card</i>	Match credit cards.		
	<i>ssn</i>	Match social security numbers.		
	<i>regexp</i>	Use a regular expression to match content.		
	<i>file-type</i>	Match a DLP file pattern list.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>file-size</i>	Match any file over with a size over the threshold.			
	<i>watermark</i>	Look for defined file watermarks.			
	<i>encrypted</i>	Look for encrypted files.			
file-size	Match files this size or larger .	integer	Minimum value: 0 Maximum value: 4294967295	0 **	
company-identifier	Enter a company identifier watermark to match. Only watermarks that your company has placed on the files are matched.	string	Maximum length: 35		
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35		
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0	
regexp	Enter a regular expression to match (max. 255 characters).	string	Maximum length: 255		
archive	Enable/disable DLP archiving.	option	-	disable	
	Option	Description			
	<i>disable</i>	No DLP archiving.			
	<i>enable</i>	Enable full DLP archiving.			
action	Action to take with content that this DLP sensor matches.	option	-	allow	
	Option	Description			
	<i>allow</i>	Allow the content to pass through the FortiGate and do not create a log message.			
	<i>log-only</i>	Allow the content to pass through the FortiGate, but write a log message.			
	<i>block</i>	Block the content and write a log message.			
	<i>quarantine-ip</i>	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	

** Values may differ between models.

dnsfilter

This section includes syntax for the following commands:

- [config dnsfilter profile on page 102](#)
- [config dnsfilter domain-filter on page 101](#)

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
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
domain	Domain entries to be filtered.	string	Maximum length: 511	
type	DNS domain filter type.	option	-	simple

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>simple</i>	Simple domain string.		
	<i>regex</i>	Regular expression domain string.		
	<i>wildcard</i>	Wildcard domain string.		
action	Action to take for domain filter matches.	option	-	block
	Option	Description		
	<i>block</i>	Block DNS requests matching the domain filter.		
	<i>allow</i>	Allow DNS requests matching the domain filter without logging.		
	<i>monitor</i>	Allow DNS requests matching the domain filter with logging.		
status	Enable/disable this domain filter.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this domain filter.		
	<i>disable</i>	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
next
end

```

config dnsfilter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable
Parameter	Description	Option	Description	
		enable	Enable logging of all domains visited.	
		disable	Disable logging of all domains visited.	
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-	enable
Parameter	Description	Option	Description	
		enable	Enable FortiGuard SDNS rating error logging.	
		disable	Disable FortiGuard SDNS rating error logging.	
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-	enable
Parameter	Description	Option	Description	
		enable	Enable domain filtering and botnet domain logging.	
		disable	Disable domain filtering and botnet domain logging.	

Parameter	Description	Type	Size	Default						
block-action	Action to take for blocked domains.	option	-	redirect						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>block</i>	Return NXDOMAIN for blocked domains.	<i>redirect</i>	Redirect blocked domains to SDNS portal.			
Option	Description									
<i>block</i>	Return NXDOMAIN for blocked domains.									
<i>redirect</i>	Redirect blocked domains to SDNS portal.									
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.									
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>strict</i>	Enable strict safe seach for YouTube.	<i>moderate</i>	Enable moderate safe search for YouTube.			
Option	Description									
<i>strict</i>	Enable strict safe seach for YouTube.									
<i>moderate</i>	Enable moderate safe search for YouTube.									
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79							

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
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
addr-type	DNS translation type (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 address type.		
	<i>ipv6</i>	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

Parameter	Description	Type	Size	Default						
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable this DNS translation.</td></tr> <tr> <td><i>disable</i></td><td>Disable this DNS translation.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable this DNS translation.	<i>disable</i>	Disable this DNS translation.
Option	Description									
<i>enable</i>	Enable this DNS translation.									
<i>disable</i>	Disable this DNS translation.									
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	integer	Minimum value: 1 Maximum value: 128	128						

emailfilter

This section includes syntax for the following commands:

- [config emailfilter block-allow-list on page 109](#)
- [config emailfilter dnsbl on page 112](#)
- [config emailfilter iptrust on page 113](#)
- [config emailfilter bword on page 107](#)
- [config emailfilter mheader on page 111](#)
- [config emailfilter profile on page 114](#)
- [config emailfilter options on page 122](#)
- [config emailfilter fortishield on page 121](#)

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|regexp]
                set action [spam|clear]
                set where [subject|body|...]
                set language [western|simch|...]
                set score {integer}
            next
        end
    next
end
```

config emailfilter bword

Parameter	Description	Type	Size	Default
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.		
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>regexp</i>	Perl regular expression.		
action	Mark spam or good.	option	-	spam
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>thai</i>	Thai.		
	<i>spanish</i>	Spanish.		
score	Score value.	integer	Minimum value: 1 Maximum value: 99999	10

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]
                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 email-pattern {string}
            next
        end
    next
end
```

config emailfilter block-allow-list

Parameter	Description	Type	Size	Default
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.		
type	Entry type.	option	-	ip
	Option	Description		
	<i>ip</i>	By IP address.		
	<i>email</i>	By email address.		
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.		
	<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>regexp</i>	Perl regular expression.		
email-pattern	Email address pattern.	string	Maximum length: 127	

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
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.
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regexp</i>	Perl regular expression.		
action	Mark spam or good.	option	-	spam
	Option	Description		
	<i>spam</i>	Mark as spam email.		
	<i>clear</i>	Mark as good email.		

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
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
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 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
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.		
addr-type	Type of address.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 Address type.		
	<i>ipv6</i>	IPv6 Address type.		
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 profile

Configure Email Filter profiles.

```
config emailfilter profile
  Description: Configure Email Filter profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    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 hdrip [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
comment	Comment.	var-string	Maximum length: 255	
feature-set	Flow/proxy feature set.	option	-	flow
Option		Description		
		<i>flow</i> Flow feature set.		
		<i>proxy</i> Proxy feature set.		

Parameter	Description	Type	Size	Default
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.		
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-	disable
Option		Description		
		<i>disable</i> Disable logging FortiGuard spam response.		
		<i>enable</i> Enable logging FortiGuard spam response.		
spam-filtering	Enable/disable spam filtering.	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
external	Enable/disable external Email inspection.	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
options	Options.	option	-	
Option		Description		
		<i>bannedword</i> Content block.		
		<i>spambal</i> Block/allow list.		
		<i>spamfsip</i> Email IP address FortiGuard AntiSpam block list check.		
		<i>spamfssubmit</i> Add FortiGuard AntiSpam spam submission text.		
		<i>spamfschksum</i> Email checksum FortiGuard AntiSpam check.		
		<i>spamfsurl</i> Email content URL FortiGuard AntiSpam check.		
		<i>spamhelodns</i> Email helo/ehlo domain DNS check.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<code>spamraddrdns</code>	Email return address DNS check.			
	<code>spamrbl</code>	Email DNSBL & ORBL check.			
	<code>spamhdrcheck</code>	Email mime header check.			
	<code>spamfsphish</code>	Email content phishing URL FortiGuard AntiSpam check.			
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

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.		
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 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

Parameter	Description	Type	Size	Default
	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
	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
	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
	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

Parameter	Description	Type	Size	Default
	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
	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
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.			

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		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
spam-submit-txt2htm	Enable/disable conversion of text email to HTML email.	option	-	enable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		

config emailfilter 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 .	integer	Minimum value: 1 Maximum value: 30	7

endpoint-control

This section includes syntax for the following commands:

- [config endpoint-control fctems on page 123](#)

config endpoint-control fctems

Configure FortiClient Enterprise Management Server (EMS) entries.

```
config endpoint-control fctems
  Description: Configure FortiClient Enterprise Management Server (EMS) entries.
  edit <name>
    set fortinetone-cloud-authentication [enable|disable]
    set server {string}
    set https-port {integer}
    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 cloud-server-type [production|alpha|...]
    set capabilities {option1}, {option2}, ...
    set call-timeout {integer}
    set websocket-override [disable|enable]
    set preserve-ssl-session [enable|disable]
  next
end
```

config endpoint-control fctems

Parameter	Description		Type	Size	Default						
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.		option	-	disable						
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr><tr><td>disable</td><td>Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr></tbody></table>		Option	Description	enable	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.	disable	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.			
Option	Description										
enable	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.										
disable	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.										
server	FortiClient EMS FQDN or IPv4 address.		string	Maximum length: 255							

Parameter	Description	Type	Size	Default						
https-port	FortiClient EMS HTTPS access port number. .	integer	Minimum value: 1 Maximum value: 65535	443						
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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												
cloud-server-type	Cloud server type.	option	-	production												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>production</i></td><td>Production FortiClient EMS Cloud Controller.</td></tr> <tr> <td><i>alpha</i></td><td>Alpha FortiClient EMS Cloud Controller.</td></tr> <tr> <td><i>beta</i></td><td>Beta FortiClient EMS Cloud Controller.</td></tr> </tbody> </table>	Option	Description	<i>production</i>	Production FortiClient EMS Cloud Controller.	<i>alpha</i>	Alpha FortiClient EMS Cloud Controller.	<i>beta</i>	Beta FortiClient EMS Cloud Controller.							
Option	Description															
<i>production</i>	Production FortiClient EMS Cloud Controller.															
<i>alpha</i>	Alpha FortiClient EMS Cloud Controller.															
<i>beta</i>	Beta FortiClient EMS Cloud Controller.															
capabilities	List of EMS capabilities.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>fabric-auth</i></td><td>Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.</td></tr> <tr> <td><i>silent-approval</i></td><td>Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.</td></tr> <tr> <td><i>websocket</i></td><td>Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.</td></tr> <tr> <td><i>websocket-malware</i></td><td>Allow this FortiGate unit to request malware hash notifications over websocket.</td></tr> <tr> <td><i>push-ca-certs</i></td><td>Enable/disable syncing deep inspection certificates with EMS.</td></tr> </tbody> </table>	Option	Description	<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.	<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.	<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.			
Option	Description															
<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.															
<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.															
<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.															
<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.															
<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.															
call-timeout	FortiClient EMS call timeout in seconds .	integer	Minimum value: 1 Maximum value: 180	30												
websocket-override	Enable/disable override behavior for how this FortiGate unit connects to EMS using a WebSocket connection.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</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>enable</i></td><td>Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).	<i>enable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.									
Option	Description															
<i>disable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).															
<i>enable</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												

Parameter	Description	Type	Size	Default
Option	Description			
<i>enable</i>	Allow preservation of EMS SSL session connection.			
<i>disable</i>	Don't allow preservation of EMS SSL session connection.			

extender

This section includes syntax for the following commands:

- [config extender extender-info on page 127](#)
- [config extender lte-carrier-by-mcc-mnc on page 128](#)
- [config extender modem-status on page 128](#)
- [config extender lte-carrier-list on page 128](#)
- [config extender sys-info on page 127](#)

config extender sys-info

Display detailed extender system information.

```
config extender sys-info
  Description: Display detailed extender system information.
  set <sn> {string}
end
```

config extender sys-info

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

config extender extender-info

Display extender struct information.

```
config extender extender-info
  Description: Display extender struct information.
  set <sn> {string}
end
```

config extender extender-info

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

config extender modem-status

Display detailed extender modem status.

```
config extender modem-status
  Description: Display detailed extender modem status.
  set <sn> {string}
end
```

config extender modem-status

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

config extender lte-carrier-list

Display extender modem carrier list.

```
config extender lte-carrier-list
  Description: Display extender modem carrier list.
  set <sn> {string}
end
```

config extender lte-carrier-list

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

config extender lte-carrier-by-mcc-mnc

Display extender modem carrier based on MCC and MNC.

```
config extender lte-carrier-by-mcc-mnc
  Description: Display extender modem carrier based on MCC and MNC.
  set <sn> {string}
end
```

config extender lte-carrier-by-mcc-mnc

Parameter	Description	Type	Size	Default
<sn>	extender serial number.	string	Maximum length: -1	

extender-controller

This section includes syntax for the following commands:

- [config extender-controller dataplan on page 129](#)
- [config extender-controller extender on page 131](#)

config extender-controller dataplan

FortiExtender dataplan configuration.

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

config extender-controller dataplan

Parameter	Description	Type	Size	Default
modem-id	Dataplan's modem specifics, if any.	option	-	all
Option	Description			
<i>modem1</i>	Modem one.			
<i>modem2</i>	Modem two.			
<i>all</i>	All modems.			
type	Type preferences configuration.	option	-	generic

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>carrier</i>	Assign by SIM carrier.		
	<i>slot</i>	Assign to SIM slot 1 or 2.		
	<i>iccid</i>	Assign to a specific SIM by ICCID.		
	<i>generic</i>	Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.		
slot	SIM slot configuration.	option	-	
	Option	Description		
	<i>sim1</i>	Sim slot one.		
	<i>sim2</i>	Sim slot two.		
iccid	ICCID configuration.	string	Maximum length: 31	
carrier	Carrier configuration.	string	Maximum length: 31	
apn	APN configuration.	string	Maximum length: 63	
auth-type	Authentication type.	option	-	none
	Option	Description		
	<i>none</i>	No authentication.		
	<i>pap</i>	PAP.		
	<i>chap</i>	CHAP.		
username	Username.	string	Maximum length: 31	
password	Password.	password	Not Specified	
pdn	PDN type.	option	-	ipv4-only
	Option	Description		
	<i>ipv4-only</i>	IPv4 only PDN activation.		
	<i>ipv6-only</i>	IPv6 only PDN activation.		
	<i>ipv4-ipv6</i>	Both IPv4 and IPv6 PDN activations.		

Parameter	Description	Type	Size	Default						
signal-threshold	Signal threshold. Specify the range between 50 - 100, where 50/100 means -50/-100 dBm.	integer	Minimum value: 50 Maximum value: 100	100						
signal-period	Signal period (600 to 18000 seconds).	integer	Minimum value: 600 Maximum value: 18000	3600						
capacity	Capacity in MB .	integer	Minimum value: 0 Maximum value: 102400000	0						
monthly-fee	Monthly fee of dataplan .	integer	Minimum value: 0 Maximum value: 1000000	0						
billing-date	Billing day of the month .	integer	Minimum value: 1 Maximum value: 31	1						
overage	Enable/disable dataplan overage detection.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable dataplan overage detection.</td></tr> <tr> <td><i>enable</i></td><td>Enable dataplan overage detection.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable dataplan overage detection.	<i>enable</i>	Enable dataplan overage detection.
Option	Description									
<i>disable</i>	Disable dataplan overage detection.									
<i>enable</i>	Enable dataplan overage detection.									
preferred-subnet	Preferred subnet mask .	integer	Minimum value: 8 Maximum value: 32	32						
private-network	Enable/disable dataplan private network support.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable dataplan private network support.</td></tr> <tr> <td><i>enable</i></td><td>Enable dataplan private network support.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable dataplan private network support.	<i>enable</i>	Enable dataplan private network support.
Option	Description									
<i>disable</i>	Disable dataplan private network support.									
<i>enable</i>	Enable dataplan private network support.									

config extender-controller extender

Extender controller configuration.

```

config extender-controller extender
    Description: Extender controller configuration.
    edit <name>
        set id {string}
        set authorized [disable|enable]
        set ext-name {string}
        set description {string}
        set vdom {integer}
        set login-password {password}
        config controller-report
            Description: FortiExtender controller report configuration.
            set status [disable|enable]
            set interval {integer}
            set signal-threshold {integer}
        end
        config modem1
            Description: Configuration options for modem 1.
            set ifname {string}
            set redundant-mode [disable|enable]
            set redundant-intf {string}
            set conn-status {integer}
            set default-sim [sim1|sim2|...]
            set gps [disable|enable]
            set sim1-pin [disable|enable]
            set sim2-pin [disable|enable]
            set sim1-pin-code {password}
            set sim2-pin-code {password}
            set preferred-carrier {string}
            config auto-switch
                Description: FortiExtender auto switch configuration.
                set disconnect [disable|enable]
                set disconnect-threshold {integer}
                set disconnect-period {integer}
                set signal [disable|enable]
                set dataplan [disable|enable]
                set switch-back {option1}, {option2}, ...
                set switch-back-time {string}
                set switch-back-timer {integer}
            end
        end
        config modem2
            Description: Configuration options for modem 2.
            set ifname {string}
            set redundant-mode [disable|enable]
            set redundant-intf {string}
            set conn-status {integer}
            set default-sim [sim1|sim2|...]
            set gps [disable|enable]
            set sim1-pin [disable|enable]
            set sim2-pin [disable|enable]
            set sim1-pin-code {password}
            set sim2-pin-code {password}
            set preferred-carrier {string}
            config auto-switch
                Description: FortiExtender auto switch configuration.
                set disconnect [disable|enable]
                set disconnect-threshold {integer}

```

```

        set disconnect-period {integer}
        set signal [disable|enable]
        set dataplan [disable|enable]
        set switch-back {option1}, {option2}, ...
        set switch-back-time {string}
        set switch-back-timer {integer}
    end
end
next
end

```

config extender-controller extender

Parameter	Description	Type	Size	Default
id	FortiExtender serial number.	string	Maximum length: 19	
authorized	FortiExtender Administration (enable or disable).	option	-	disable
	Option	Description		
	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.		
	<i>enable</i>	Controller is configured to provide service to this FortiExtender.		
ext-name	FortiExtender name.	string	Maximum length: 31	
description	Description.	string	Maximum length: 255	
vdom	VDOM	integer	Minimum value: 0 Maximum value: 4294967295	0
login-password	FortiExtender login password.	password	Not Specified	

config controller-report

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

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

config modem1

Parameter	Description	Type	Size	Default
ifname	FortiExtender interface name.	string	Maximum length: 15	
redundant-mode	FortiExtender mode.	option	-	disable
Option		Description		
		<i>disable</i> Disable interface redundancy.		
		<i>enable</i> Enable interface redundancy.		
redundant-intf	Redundant interface.	string	Maximum length: 15	
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0
default-sim	Default SIM selection.	option	-	sim1
Option		Description		
		<i>sim1</i> Use SIM #1 by default.		
		<i>sim2</i> Use SIM #2 by default.		
		<i>carrier</i> Assign default SIM based on carrier.		
		<i>cost</i> Assign default SIM based on cost.		
gps	FortiExtender GPS enable/disable.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable GPS.		
	<i>enable</i>	Enable GPS.		
sim1-pin	SIM #1 PIN status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SIM #1 pin.		
	<i>enable</i>	Enable SIM #1 pin.		
sim2-pin	SIM #2 PIN status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SIM #2 pin.		
	<i>enable</i>	Enable SIM #2 pin.		
sim1-pin-code	SIM #1 PIN password.	password	Not Specified	
sim2-pin-code	SIM #2 PIN password.	password	Not Specified	
preferred-carrier	Preferred carrier.	string	Maximum length: 31	

config auto-switch

Parameter	Description	Type	Size	Default
disconnect	Auto switch by disconnect.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable switching of SIM card based on cellular disconnections.		
	<i>enable</i>	Enable switching of SIM card based on cellular disconnections.		
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 0 Maximum value: 4294967295	3

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

config modem2

Parameter	Description	Type	Size	Default						
ifname	FortiExtender interface name.	string	Maximum length: 15							
redundant-mode	FortiExtender mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable interface redundancy.</td></tr> <tr> <td><i>enable</i></td><td>Enable interface redundancy.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable interface redundancy.	<i>enable</i>	Enable interface redundancy.			
Option	Description									
<i>disable</i>	Disable interface redundancy.									
<i>enable</i>	Enable interface redundancy.									

Parameter	Description	Type	Size	Default										
redundant-intf	Redundant interface.	string	Maximum length: 15											
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0										
default-sim	Default SIM selection.	option	-	sim1										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>sim1</i></td><td>Use SIM #1 by default.</td></tr> <tr> <td><i>sim2</i></td><td>Use SIM #2 by default.</td></tr> <tr> <td><i>carrier</i></td><td>Assign default SIM based on carrier.</td></tr> <tr> <td><i>cost</i></td><td>Assign default SIM based on cost.</td></tr> </tbody> </table>	Option	Description	<i>sim1</i>	Use SIM #1 by default.	<i>sim2</i>	Use SIM #2 by default.	<i>carrier</i>	Assign default SIM based on carrier.	<i>cost</i>	Assign default SIM based on cost.			
Option	Description													
<i>sim1</i>	Use SIM #1 by default.													
<i>sim2</i>	Use SIM #2 by default.													
<i>carrier</i>	Assign default SIM based on carrier.													
<i>cost</i>	Assign default SIM based on cost.													
gps	FortiExtender GPS enable/disable.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable GPS.</td></tr> <tr> <td><i>enable</i></td><td>Enable GPS.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable GPS.	<i>enable</i>	Enable GPS.							
Option	Description													
<i>disable</i>	Disable GPS.													
<i>enable</i>	Enable GPS.													
sim1-pin	SIM #1 PIN status.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable SIM #1 pin.</td></tr> <tr> <td><i>enable</i></td><td>Enable SIM #1 pin.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SIM #1 pin.	<i>enable</i>	Enable SIM #1 pin.							
Option	Description													
<i>disable</i>	Disable SIM #1 pin.													
<i>enable</i>	Enable SIM #1 pin.													
sim2-pin	SIM #2 PIN status.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable SIM #2 pin.</td></tr> <tr> <td><i>enable</i></td><td>Enable SIM #2 pin.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable SIM #2 pin.	<i>enable</i>	Enable SIM #2 pin.							
Option	Description													
<i>disable</i>	Disable SIM #2 pin.													
<i>enable</i>	Enable SIM #2 pin.													
sim1-pin-code	SIM #1 PIN password.	password	Not Specified											
sim2-pin-code	SIM #2 PIN password.	password	Not Specified											
preferred-carrier	Preferred carrier.	string	Maximum length: 31											

config auto-switch

Parameter	Description	Type	Size	Default
disconnect	Auto switch by disconnect.	option	-	disable
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 0 Maximum value: 4294967295	3
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600
signal	Automatically switch based on signal strength.	option	-	disable
dataplan	Automatically switch based on data usage.	option	-	disable
switch-back	Auto switch with switch back multi-options.	option	-	
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time .	integer	Minimum value: 3600 Maximum value: 2147483647	86400

file-filter

This section includes syntax for the following commands:

- [config file-filter profile on page 139](#)

config file-filter profile

Configure file-filter profiles.

```
config file-filter profile
  Description: Configure file-filter profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    set log [disable|enable]
    set extended-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
comment	Comment.	var-string	Maximum length: 255	
feature-set	Flow/proxy feature set.	option	-	flow
		Option	Description	
		flow	Flow feature set.	
		proxy	Proxy feature set.	
replacemsg-group	Replacement message group	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
log	Enable/disable file-filter logging.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
extended-log	Enable/disable file-filter extended logging.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable extended logging.		
	<i>enable</i>	Enable extended 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
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.)		

Parameter	Description	Type	Size	Default
action	Action taken for matched file.	option	-	log-only
	Option	Description		
	<i>log-only</i>	Allow the content and write a log message.		
	<i>block</i>	Block the content and write a log message.		
direction	Traffic direction. (HTTP, FTP, SSH, CIFS 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 acl6](#) on page 427
- [config firewall vipgrp](#) on page 257
- [config firewall access-proxy6](#) on page 284
- [config firewall shaping-profile](#) on page 391
- [config firewall iprope appctrl status](#) on page 435
- [config firewall security-policy](#) on page 361
- [config firewall internet-service-extension](#) on page 170
- [config firewall central-snat-map](#) on page 428
- [config firewall internet-service-list](#) on page 177
- [config firewall vendor-mac-summary](#) on page 180
- [config firewall multicast-address](#) on page 148
- [config firewall shaper per-ip-shaper](#) on page 182
- [config firewall shaping-policy](#) on page 386
- [config firewall proute](#) on page 435
- [config firewall ip-translation](#) on page 432
- [config firewall proxy-addrgrp](#) on page 188
- [config firewall ssh local-ca](#) on page 259
- [config firewall service category](#) on page 160
- [config firewall iprope appctrl list](#) on page 435
- [config firewall multicast-address6](#) on page 154
- [config firewall internet-service-name](#) on page 168
- [config firewall dnstranslation](#) on page 405
- [config firewall iprope list](#) on page 435
- [config firewall ippool6](#) on page 194
- [config firewall service group](#) on page 164
- [config firewall internet-service-custom](#) on page 172
- [config firewall city](#) on page 165
- [config firewall addrgrp6](#) on page 157
- [config firewall sniffer](#) on page 420
- [config firewall schedule onetime](#) on page 189
- [config firewall policy](#) on page 368
- [config firewall ssh setting](#) on page 260
- [config firewall internet-service-ipbl-vendor](#) on page 176
- [config firewall internet-service-append](#) on page 175
- [config firewall multicast-policy6](#) on page 408
- [config firewall address](#) on page 144
- [config firewall internet-service-custom-group](#) on page 176
- [config firewall ssl setting](#) on page 430
- [config firewall ssl-server](#) on page 357

-
- config firewall shaper traffic-shaper on page 180
 - config firewall DoS-policy6 on page 418
 - config firewall interface-policy on page 410
 - config firewall shaper traffic on page 184
 - config firewall proute6 on page 436
 - config firewall ippool on page 192
 - config firewall vipgrp6 on page 258
 - config firewall ssh local-key on page 258
 - config firewall internet-service-reputation on page 172
 - config firewall traffic-class on page 386
 - config firewall ipmacbinding setting on page 303
 - config firewall profile-protocol-options on page 304
 - config firewall ssl-ssh-profile on page 328
 - config firewall schedule recurring on page 190
 - config firewall local-in-policy6 on page 395
 - config firewall wildcard-fqdn custom on page 158
 - config firewall ipv6-eh-filter on page 433
 - config firewall acl on page 426
 - config firewall internet-service on page 167
 - config firewall local-in-policy on page 393
 - config firewall shaper per-ip on page 184
 - config firewall schedule group on page 191
 - config firewall ssh host-key on page 261
 - config firewall multicast-policy on page 406
 - config firewall country on page 166
 - config firewall internet-service-owner on page 177
 - config firewall address6 on page 151
 - config firewall proxy-policy on page 398
 - config firewall internet-service-ipbl-reason on page 177
 - config firewall vendor-mac on page 179
 - config firewall access-proxy on page 265
 - config firewall internet-service-sld on page 176
 - config firewall ipmacbinding table on page 304
 - config firewall service custom on page 160
 - config firewall internet-service-addition on page 174
 - config firewall identity-based-route on page 360
 - config firewall ldb-monitor on page 195
 - config firewall ttl-policy on page 397
 - config firewall DoS-policy on page 416
 - config firewall vip on page 197
 - config firewall region on page 166
 - config firewall decrypted-traffic-mirror on page 359
 - config firewall internet-service-definition on page 178
 - config firewall proxy-address on page 184
 - config firewall access-proxy-ssh-client-cert on page 263

- config firewall internet-service-group on page 169
- config firewall vip6 on page 228
- config firewall access-proxy-virtual-host on page 262
- config firewall auth-portal on page 361
- config firewall addrgrp on page 155
- config firewall wildcard-fqdn group on page 159
- config firewall profile-group on page 355
- config firewall internet-service-botnet on page 179
- config firewall interface-policy6 on page 413
- config firewall address6-template on page 150

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 sub-type [sdn|clearpass-spt|...]
        set clearpass-spt [unknown|healthy|...]
        set macaddr <macaddr1>, <macaddr2>, ...
        set start-ip {ipv4-address-any}
        set end-ip {ipv4-address-any}
        set fqdn {string}
        set country {string}
        set wildcard-fqdn {string}
        set cache-ttl {integer}
        set wildcard {ipv4-classnet-any}
        set sdn {string}
        set fssso-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 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
next
end
set allow-routing [enable|disable]
set fabric-object [enable|disable]
next
end

```

config firewall address

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
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>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.		
<i>mac</i>		Range of MAC addresses.		
sub-type	Sub-type of address.	option	-	sdn
Option		Description		
<i>sdn</i>		SDN address.		
<i>clearpass-spt</i>		ClearPass SPT (System Posture Token) address.		
<i>fss0</i>		FSSO address.		
<i>ems-tag</i>		FortiClient EMS tag.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>swc-tag</i>	Switch Controller NAC policy tag.		
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown
	Option	Description		
	<i>unknown</i>	UNKNOWN.		
	<i>healthy</i>	HEALTHY.		
	<i>quarantine</i>	QUARANTINE.		
	<i>checkup</i>	CHECKUP.		
	<i>transient</i>	TRANSIENT.		
	<i>infected</i>	INFECTED.		
macaddr <macaddr>	Multiple MAC address ranges. MAC address ranges <start>[-<end>] separated by space.	string	Maximum length: 127	
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	
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	
fssouser-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
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				
<i>ip</i> IP address.				
<i>mac</i> MAC address				
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
Option				
<i>private</i> Collect private addresses only.				
<i>public</i> Collect public addresses only.				
<i>all</i> Collect both public and private addresses.				

Parameter	Description	Type	Size	Default
node-ip-only	Enable/disable collection of node addresses only in Kubernetes.	option	-	disable
	Option	Description		
	enable	Enable collection of node addresses only in Kubernetes.		
	disable	Disable collection of node addresses only in Kubernetes.		
obj-id	Object ID for NSX.	var-string	Maximum length: 255	
allow-routing	Enable/disable use of this address in the static route configuration.	option	-	disable
	Option	Description		
	enable	Enable use of this address in the static route configuration.		
	disable	Disable use of this address in the static route configuration.		
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		

config tagging

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

config firewall multicast-address

Configure multicast addresses.

```
config firewall multicast-address
  Description: Configure multicast addresses.
  edit <name>
    set type {multicastrange|broadcastmask}
    set subnet {ipv4-classnet-any}
    set start-ip {ipv4-address-any}
    set end-ip {ipv4-address-any}
    set comment {var-string}
    set associated-interface {string}
```

```

set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
next
end
next
end

```

config firewall multicast-address

Parameter	Description	Type	Size	Default
type	Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.	option	-	multicastrange
	Option	Description		
	<i>multicastrange</i>	Multicast range.		
	<i>broadcastmask</i>	Broadcast IP/mask.		
subnet	Broadcast address and subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
start-ip	First IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
end-ip	Final IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
comment	Comment.	var-string	Maximum length: 255	
associated-interface	Interface associated with the address object. When setting up a policy, only addresses associated with this interface are available.	string	Maximum length: 35	
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0

config tagging

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

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

config firewall address6-template

Configure IPv6 address templates.

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

config firewall address6-template

Parameter	Description	Type	Size	Default
ip6	IPv6 address prefix.	ipv6-network	Not Specified	::/0
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6	0
fabric-object	Security Fabric global object setting.	option	-	disable
Option	Description			
enable	Object is set as a security fabric-wide global object.			
disable	Object is local to this security fabric member.			

config subnet-segment

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

config values

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

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 macaddr <macaddr1>, <macaddr2>, ...
    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}
set template {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 fabric-object [enable|disable]
next
end

```

config firewall address6

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-000000000000
type	Type of IPv6 address object .	option	-	ipprefix
Option		Description		
		<i>ipprefix</i> Uses the IP prefix to define a range of IPv6 addresses.		
		<i>iprange</i> Range of IPv6 addresses between two specified addresses (inclusive).		
		<i>fqdn</i> Fully qualified domain name.		
		<i>geography</i> IPv6 addresses from a specified country.		
		<i>dynamic</i> Dynamic address object for SDN.		
		<i>template</i> Template.		
		<i>mac</i> Range of MAC addresses.		
macaddr <macaddr>	Multiple MAC address ranges. MAC address ranges <start>[-<end>] separated by space.	string	Maximum length: 127	
sdn	SDN.	string	Maximum length: 35	
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx).	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default						
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::						
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::						
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						
color	Integer value to determine the color of the icon in the GUI .	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							
template	IPv6 address template.	string	Maximum length: 63							
host-type	Host type.	option	-	any						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>any</i></td><td>Wildcard.</td></tr> <tr> <td><i>specific</i></td><td>Specific host address.</td></tr> </tbody> </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	::						
fabric-object	Security Fabric global object setting.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 tagging

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

config subnet-segment

Parameter	Description	Type	Size	Default
type	Subnet segment type.	option	-	any
Option		Description		
		any Wildcard.		
		specific Specific subnet segment address.		
value	Subnet segment value.	string	Maximum length: 35	

config firewall multicast-address6

Configure IPv6 multicast address.

```
config firewall multicast-address6
    Description: Configure IPv6 multicast address.
    edit <name>
        set ip6 {ipv6-network}
        set comment {var-string}
        set color {integer}
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
    next
end
```

config firewall multicast-address6

Parameter	Description	Type	Size	Default
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx).	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

config tagging

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

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

config firewall addrgrp

Parameter	Description	Type	Size	Default
type	Address group type.	option	-	default
	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
	Option	Description		
	<i>default</i>	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-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
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
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.		
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
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>, ...
        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
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 .	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	
fabric-object	Security Fabric global object setting.	option	-	disable
Option	Description			
enable	Object is set as a security fabric-wide global object.			
disable	Object is local to this security fabric member.			

config tagging

Parameter	Description	Type	Size	Default
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag 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
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
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
comment	Comment.	var-string	Maximum length: 255	

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
comment	Comment.	var-string	Maximum length: 255	
fabric-object	Security Fabric global object setting.	option	-	disable
Option		Description		
		enable	Object is set as a security fabric-wide global object.	
		disable	Object is local to this security fabric member.	

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 helper [auto|disable|...]
    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 visibility [enable|disable]
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
proxy	Enable/disable web proxy service.	option	-	disable
	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
	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.		
helper	Helper name.	option	-	auto
	Option	Description		
	<i>auto</i>	Automatically select helper based on protocol and port.		
	<i>disable</i>	Disable helper.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ftp</i>	FTP.		
	<i>tftp</i>	TFTP.		
	<i>ras</i>	RAS.		
	<i>h323</i>	H323.		
	<i>tns</i>	TNS.		
	<i>mms</i>	MMS.		
	<i>sip</i>	SIP.		
	<i>pptp</i>	PPTP.		
	<i>rtsp</i>	RTSP.		
	<i>dns-udp</i>	DNS UDP.		
	<i>dns-tcp</i>	DNS TCP.		
	<i>pmap</i>	PMAP.		
	<i>rsh</i>	RSH.		
	<i>dcerpc</i>	DCERPC.		
	<i>mgcp</i>	MGCP.		
iprange	Start and end of the IP range associated with service.	user	Not Specified	
fqdn	Fully qualified domain name.	string	Maximum length: 255	
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	

Parameter	Description	Type	Size	Default
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 .	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 .	integer	Minimum value: 0 Maximum value: 86400	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds .	integer	Minimum value: 0 Maximum value: 300	0
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds .	integer	Minimum value: 5 Maximum value: 300	0
udp-idle-timer	UDP half close timeout .	integer	Minimum value: 0 Maximum value: 86400	0
session-ttl	Session TTL .	user	Not Specified	
check-reset-range	Configure the type of ICMP error message verification.	option	-	default
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

Parameter	Description	Type	Size	Default
visibility	Enable/disable the visibility of the service on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Show in service selection.		
	<i>disable</i>	Hide from service selection.		
app-service-type	Application service type.	option	-	disable
	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
	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
proxy	Enable/disable web proxy service group.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
member <name>	Service objects contained within the group. Address 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
	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 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
name	City name.	string	Maximum length: 63	

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

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

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 singularity {integer}
    set obsolete {integer}
  next
end
```

config firewall internet-service

Parameter	Description	Type	Size	Default								
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><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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.											
database	Database name this Internet Service belongs to.	option	-	isdb								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>isdb</td><td>Internet Service Database.</td></tr><tr><td>irdb</td><td>Internet RRR Database.</td></tr></tbody></table>	Option	Description	isdb	Internet Service Database.	irdb	Internet RRR Database.					
Option	Description											
isdb	Internet Service Database.											
irdb	Internet RRR Database.											

Parameter	Description	Type	Size	Default
ip-range-number	Number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
extra-ip-range-number	Extra number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-number	Total number of IP addresses.	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-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
type	Internet Service name type.	option	-	default

Parameter	Description	Type	Size	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-group

Configure group of Internet Service.

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

config firewall internet-service-group

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

Parameter	Description	Type	Size	Default
direction	How this service may be used (source, destination or both).	option	-	both
	Option	Description		
	<i>source</i>	As source when applied.		
	<i>destination</i>	As destination when applied.		
	<i>both</i>	Both directions when applied.		
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79	

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 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>, ...
      next
    end
    config disable-entry
      Description: Disable entries in the Internet Service database.
      edit <id>
        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: IP ranges in the disable entry.
          edit <id>
            set start-ip {ipv4-address-any}
            set end-ip {ipv4-address-any}
            next
      end
    end
  end
end
```

```

        end
    next
end
next
end

```

config firewall internet-service-extension

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

config entry

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

config port-range

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 disable-entry

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

config port-range

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 ip-range

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

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
description	Description.	string	Maximum length: 127	

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 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>, ...
            next
        end
    next
end

```

config firewall internet-service-custom

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

config port-range

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

config firewall internet-service-addition

Configure Internet Services Addition.

```
config firewall internet-service-addition
    Description: Configure Internet Services Addition.
    edit <id>
        set comment {var-string}
        config entry
            Description: Entries added to the Internet Service addition database.
            edit <id>
                set 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
next
end
```

config firewall internet-service-addition

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

config entry

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

config port-range

Parameter	Description	Type	Size	Default
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 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 match-port {integer}
  set append-port {integer}
end
```

config firewall internet-service-append

Parameter	Description	Type	Size	Default
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: 1 Maximum value: 65535	0

config firewall internet-service-custom-group

Configure custom Internet Service group.

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

config firewall internet-service-custom-group

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

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
name	Second Level Domain name.	string	Maximum length: 63	

config firewall internet-service-ipbl-vendor

IP blocklist vendor.

```
config firewall internet-service-ipbl-vendor
    Description: IP blocklist vendor.
    edit <id>
        set name {string}
    next
end
```

config firewall internet-service-ipbl-vendor

Parameter	Description	Type	Size	Default
name	IP blocklist vendor name.	string	Maximum length: 63	

config firewall internet-service-ipbl-reason

IP blocklist reason.

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

config firewall internet-service-ipbl-reason

Parameter	Description	Type	Size	Default
name	IP blocklist reason name.	string	Maximum length: 63	

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
name	Internet Service owner 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
name	Internet Service category name.	string	Maximum length: 63	

config firewall internet-service-definition

Configure Internet Service definition.

```

config firewall internet-service-definition
    Description: Configure Internet Service definition.
    edit <id>
        config entry
            Description: Protocol and port information in an Internet Service entry.
            edit <seq-num>
                set category-id {integer}
                set name {string}
                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

```

config entry

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

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

config port-range

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-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
name	Internet Service Botnet name.	string	Maximum length: 63	

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
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 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}
        set exceed-class-id {integer}
    next
end
```

config firewall shaper traffic-shaper

Parameter	Description	Type	Size	Default
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper .	integer	Minimum value: 0 Maximum value: 16776000	0
maximum-bandwidth	Upper bandwidth limit enforced by this shaper . 0 means no limit.	integer	Minimum value: 0 Maximum value: 16776000	0
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps
Option		Description		
<i>kbps</i>		Kilobits per second.		
<i>mbps</i>		Megabits per second.		
<i>gbps</i>		Gigabits per second.		
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-	high
Option		Description		
<i>low</i>		Low priority.		
<i>medium</i>		Medium priority.		
<i>high</i>		High priority.		
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

Parameter	Description	Type	Size	Default
	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 multi-stage marking. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000	0
exceed-dscp	DSCP mark for traffic in [guaranteed-bandwidth, exceed-bandwidth].	user	Not Specified	
maximum-dscp	DSCP mark for traffic in [exceed-bandwidth, maximum-bandwidth].	user	Not Specified	
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 Maximum value: 100	0
exceed-class-id	Class ID for traffic in [guaranteed-bandwidth, maximum-bandwidth].	integer	Minimum value: 0 Maximum value: 4294967295	0

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
max-bandwidth	Upper bandwidth limit enforced by this shaper . 0 means no limit.	integer	Minimum value: 0 Maximum value: 16776000	0
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps
Option		Description		
		<i>kbps</i> Kilobits per second.		
		<i>mbps</i> Megabits per second.		
		<i>gbps</i> Gigabits per second.		
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper . 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0
max-concurrent-tcp-session	Maximum number of concurrent TCP sessions allowed by this shaper . 0 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 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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting forward (original) traffic DiffServ.		
	<i>disable</i>	Disable setting forward (original) traffic DiffServ.		
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.		
	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.		
diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified	
diffservcode-rev	Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified	

config firewall shaper traffic

Shared traffic shapers.

```
config firewall shaper traffic
    Description: Shared traffic shapers.
end
```

config firewall shaper per-ip

Per-IP traffic shapers.

```
config firewall shaper per-ip
    Description: Per-IP traffic shapers.
end
```

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 category <id1>, <id2>, ...
set method {option1}, {option2}, ...
set ua {option1}, {option2}, ...
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}
next
end

```

config firewall proxy-address

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
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>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.		
host	Address object for the host.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
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.			
category <id>	FortiGuard category ID. Fortiguard category id.	integer	Minimum value: 0 Maximum value: 4294967295	
method	HTTP request methods to be used.	option	-	
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	-	
Option	Description			
<i>chrome</i>	Google Chrome.			
<i>ms</i>	Microsoft Internet Explorer or EDGE.			
<i>firefox</i>	Mozilla Firefox.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>safari</i>	Apple Safari.		
	<i>other</i>	Other browsers.		
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
	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 .	integer	Minimum value: 0 Maximum value: 32	0
comment	Optional comments.	var-string	Maximum length: 255	

config header-group

Parameter	Description	Type	Size	Default
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		
	<i>disable</i>	Case insensitive in pattern.		
	<i>enable</i>	Case sensitive in pattern.		

config tagging

Parameter	Description	Type	Size	Default
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
type	Source or destination address group type.	option	-	src
Parameter	Description	Type	Size	Default
	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	

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comment	Optional comments.	var-string	Maximum length: 255	

config tagging

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

config firewall schedule onetime

Onetime schedule configuration.

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

config firewall schedule onetime

Parameter	Description	Type	Size	Default
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	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
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
Option	Description			
<i>sunday</i>	Sunday.			
<i>monday</i>	Monday.			
<i>tuesday</i>	Tuesday.			
<i>wednesday</i>	Wednesday.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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 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
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 ippool

Configure IPv4 IP pools.

```
config firewall ippool
  Description: Configure IPv4 IP pools.
  edit <name>
    set type [overload|one-to-one|...]
    set startip {ipv4-address-any}
    set endip {ipv4-address-any}
    set startport {integer}
    set endport {integer}
    set source-startip {ipv4-address-any}
    set source-endip {ipv4-address-any}
    set block-size {integer}
    set port-per-user {integer}
    set num-blocks-per-user {integer}
    set pba-timeout {integer}
    set permit-any-host [disable|enable]
    set arp-reply [disable|enable]
    set arp-intf {string}
    set associated-interface {string}
    set comments {var-string}
    set nat64 [disable|enable]
    set add-nat64-route [disable|enable]
  next
end
```

config firewall ippool

Parameter	Description	Type	Size	Default
type	IP pool type (overload, one-to-one, fixed port range, or port block allocation).	option	-	overload
	Option	Description		
<i>overload</i>	IP addresses in the IP pool can be shared by clients.			
<i>one-to-one</i>	One to one mapping.			
<i>fixed-port-range</i>	Fixed port range.			
<i>port-block-allocation</i>	Port block allocation.			

Parameter	Description	Type	Size	Default
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
startport	First port number (inclusive) in the range for the address pool (Default: 5117).	integer	Minimum value: 5117 Maximum value: 65533	5117
endport	Final port number (inclusive) in the range for the address pool (Default: 65533).	integer	Minimum value: 5117 Maximum value: 65533	65533
source-startip	First IPv4 address (inclusive) in the range of the source addresses to be translated (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
source-endip	Final IPv4 address (inclusive) in the range of the source addresses to be translated (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
block-size	Number of addresses in a block .	integer	Minimum value: 64 Maximum value: 4096	128
port-per-user	Number of port for each user .	integer	Minimum value: 32 Maximum value: 60416	0
num-blocks-per-user	Number of addresses blocks that can be used by a user .	integer	Minimum value: 1 Maximum value: 128	8
pba-timeout	Port block allocation timeout (seconds).	integer	Minimum value: 3 Maximum value: 300	30
permit-any-host	Enable/disable full cone NAT.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable full cone NAT.		
	<i>enable</i>	Enable full cone NAT.		
arp-reply	Enable/disable replying to ARP requests when an IP Pool is added to a policy .	option	-	enable
	Option	Description		
	<i>disable</i>	Disable ARP reply.		
	<i>enable</i>	Enable ARP reply.		
arp-intf	Select an interface from available options that will reply to ARP requests. (If blank, any is selected).	string	Maximum length: 15	
associated-interface	Associated interface name.	string	Maximum length: 15	
comments	Comment.	var-string	Maximum length: 255	
nat64	Enable/disable NAT64.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable DNAT64.		
	<i>enable</i>	Enable DNAT64.		
add-nat64-route	Enable/disable adding NAT64 route.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable adding NAT64 route.		
	<i>enable</i>	Enable adding NAT64 route.		

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
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
Option	Description			
<i>disable</i>	Disable NAT46.			
<i>enable</i>	Enable NAT46.			
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable
Option	Description			
<i>disable</i>	Disable adding NAT46 route.			
<i>enable</i>	Enable adding NAT46 route.			

config firewall ldb-monitor

Configure server load balancing health monitors.

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

end

config firewall ldb-monitor

Parameter	Description	Type	Size	Default
type	Select the Monitor type used by the health check monitor to check the health of the server (PING TCP HTTP HTTPS DNS).	option	-	
	Option	Description		
	<i>ping</i>	PING health monitor.		
	<i>tcp</i>	TCP-connect health monitor.		
	<i>http</i>	HTTP-GET health monitor.		
	<i>https</i>	HTTP-GET health monitor with SSL.		
	<i>dns</i>	DNS health monitor.		
interval	Time between health checks .	integer	Minimum value: 5 Maximum value: 65535	10
timeout	Time to wait to receive response to a health check from a server. Reaching the timeout means the health check failed .	integer	Minimum value: 1 Maximum value: 255	2
retry	Number health check attempts before the server is considered down .	integer	Minimum value: 1 Maximum value: 255	3
port	Service port used to perform the health check. If 0, health check monitor inherits port configured for the server .	integer	Minimum value: 0 Maximum value: 65535	0
src-ip	Source IP for ldb-monitor.	ipv4-address	Not Specified	0.0.0.0
http-get	URL used to send a GET request to check the health of an HTTP server.	string	Maximum length: 255	
http-match	String to match the value expected in response to an HTTP-GET request.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
http-max-redirects	The maximum number of HTTP redirects to be allowed.	integer	Minimum value: 0 Maximum value: 5	0
dns-protocol	Select the protocol used by the DNS health check monitor to check the health of the server (UDP TCP).	option	-	udp
Option	Description			
udp	UDP.			
tcp	TCP.			
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255	
dns-match-ip	Response IP expected from DNS server.	ipv4-address	Not Specified	0.0.0.0

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|load-balance|...]
    set dns-mapping-ttl {integer}
    set ldb-method [static|round-robin|...]
    set src-filter <range1>, <range2>, ...
    set service <name1>, <name2>, ...
    set extip {user}
    set extaddr <name1>, <name2>, ...
    set nat44 [disable|enable]
    set nat46 [disable|enable]
    set add-nat46-route [disable|enable]
    set mappedip <range1>, <range2>, ...
    set mapped-addr {string}
    set extintf {string}
    set arp-reply [disable|enable]
    set server-type [http|https|...]
    set http-redirect [enable|disable]
    set persistence [none|http-cookie|...]
    set nat-source-vip [disable|enable]
    set portforward [disable|enable]
    set status [disable|enable]
    set protocol [tcp|udp|...]
    set extport {user}
    set mappedport {user}
```

```

set gratuitous-arp-interval {integer}
set srcintf-filter <interface-name1>, <interface-name2>, ...
set portmapping-type [1-to-1|m-to-n]
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 http-host {string}
        set max-connections {integer}
        set monitor <name1>, <name2>, ...
        set client-ip {user}
    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-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 {string}
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-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-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 monitor <name1>, <name2>, ...
set max-embryonic-connections {integer}
set color {integer}
set ipv6-mappedip {user}
set ipv6-mappedport {user}
next
end

```

config firewall vip

Parameter	Description	Type	Size	Default
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 a static NAT, load balance, server load balance, access proxy, DNS translation, or FQDN VIP.	option	-	static-nat
Option	Description			
<i>static-nat</i>	Static NAT.			

Parameter	Description	Type	Size	Default
Option				
<i>load-balance</i>				Load balance.
<i>server-load-balance</i>				Server load balance.
<i>dns-translation</i>				DNS translation.
<i>fqdn</i>				Fully qualified domain name.
<i>access-proxy</i>				Access proxy.
dns-mapping-ttl	DNS mapping TTL .	integer	Minimum value: 0 Maximum value: 604800	0
ldb-method	Method used to distribute sessions to real servers.	option	-	static
Option				
<i>static</i>				Distribute to server based on source IP.
<i>round-robin</i>				Distribute to server based round robin order.
<i>weighted</i>				Distribute to server based on weight.
<i>least-session</i>				Distribute to server with lowest session count.
<i>least-rtt</i>				Distribute to server with lowest Round-Trip-Time.
<i>first-alive</i>				Distribute to the first server that is alive.
<i>http-host</i>				Distribute to server based on host field in HTTP header.
src-filter <range>	Source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y.y). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79	
service <name>	Service name. Service name.	string	Maximum length: 79	
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	
extaddr <name>	External FQDN address name. Address name.	string	Maximum length: 79	
nat44	Enable/disable NAT44.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable NAT44.		
	<i>enable</i>	Enable NAT44.		
nat46	Enable/disable NAT46.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable NAT46.		
	<i>enable</i>	Enable NAT46.		
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable adding NAT46 route.		
	<i>enable</i>	Enable adding NAT46 route.		
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	
mapped-addr	Mapped FQDN address name.	string	Maximum length: 79	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35	
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable ARP reply.		
	<i>enable</i>	Enable ARP reply.		
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-	
	Option	Description		
	<i>http</i>	HTTP.		
	<i>https</i>	HTTPS.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>imaps</i>	IMAPS.		
	<i>pop3s</i>	POP3S.		
	<i>smtpls</i>	SMTPLS.		
	<i>ssl</i>	SSL.		
	<i>tcp</i>	TCP.		
	<i>udp</i>	UDP.		
	<i>ip</i>	IP.		
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-	disable
	Option	Description		
	<i>enable</i>	Enable redirection of HTTP to HTTPS.		
	<i>disable</i>	Disable redirection of HTTP to HTTPS.		
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>http-cookie</i>	HTTP cookie.		
	<i>ssl-session-id</i>	SSL session ID.		
nat-source-vip	Enable/disable forcing the source NAT mapped IP to the external IP for all traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.		
	<i>enable</i>	Force the source NAT mapped IP to the external IP for all traffic.		
portforward	Enable/disable port forwarding.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable port forward.		
	<i>enable</i>	Enable port forward.		

Parameter	Description	Type	Size	Default										
status	Enable/disable VIP.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable the VIP.</td></tr> <tr> <td><i>enable</i></td><td>Enable the VIP.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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										
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										
srcintf-filter <interface-name>	Interfaces to which the VIP applies. Separate the names with spaces. Interface name.	string	Maximum length: 79											
portmapping-type	Port mapping type.	option	-	1-to-1										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>1-to-1</i></td><td>One to one.</td></tr> <tr> <td><i>m-to-n</i></td><td>Many to many.</td></tr> </tbody> </table>	Option	Description	<i>1-to-1</i>	One to one.	<i>m-to-n</i>	Many to many.							
Option	Description													
<i>1-to-1</i>	One to one.													
<i>m-to-n</i>	Many to many.													
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookie-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 virtual servers. same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option	Description		
	<i>disable</i>	Only allow HTTP cookie to match this virtual server.		
	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.		
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.		
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HTTP session multiplexing.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<code>disable</code>	Disable HTTP session multiplexing.		
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable
	Option	Description		
	<code>enable</code>	Enable adding HTTP header.		
	<code>disable</code>	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
	Option	Description		
	<code>disable</code>	Disable Outlook Web Access support.		
	<code>enable</code>	Enable Outlook Web Access support.		
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable
	Option	Description		
	<code>disable</code>	Do not add HTTP header indicating SSL offload for WebLogic server.		
	<code>enable</code>	Add HTTP header indicating SSL offload for WebLogic server.		
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable
	Option	Description		
	<code>disable</code>	Do not add HTTP header indicating SSL offload for WebSphere server.		
	<code>enable</code>	Add HTTP header indicating SSL offload for WebSphere server.		
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>half</i>	Client to FortiGate SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		
ssl-certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35	
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 SSL 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.		
	<i>custom</i>	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
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>custom</i>	Custom encryption. Use <code>ssl-server-cipher-suites</code> to select the cipher suites that are allowed.		
	<i>client</i>	Use the same encryption algorithms for both client and server sessions.		
<code>ssl-pfs</code>	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require
	Option	Description		
	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.		
	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.		
	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.		
<code>ssl-min-version</code>	Lowest SSL/TLS version acceptable from a client.	option	-	<code>tls-1.1</code>
	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.		
<code>ssl-max-version</code>	Highest SSL/TLS version acceptable from a client.	option	-	<code>tls-1.3</code>
	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.		
<code>ssl-server-min-version</code>	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
<i>client</i>	Use same value as client configuration.																	
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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-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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>enable</i></td><td>Enable.</td></tr> </tbody> </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
	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 FortiGate.	option	-	both
	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 FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30
ssl-client-session-state-max	Maximum number of client to FortiGate 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-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both
	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.		

Parameter	Description	Type	Size	Default								
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60								
ssl-server-session-state-max	Maximum number of FortiGate 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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 honour 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									

Parameter	Description	Type	Size	Default
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable
	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
	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 honour 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
	Option	Description		
	<i>disable</i>	HSTS header does not apply to subdomains.		
	<i>enable</i>	HSTS header applies to subdomains.		
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
ipv6-mappedip	Start-mapped-IPv6-address [-end mapped-IPv6-address].	user	Not Specified	

Parameter	Description	Type	Size	Default
ipv6-mappedport	IPv6 port number range on the destination network to which the external port number range is mapped.	user		Not Specified

config realservers

Parameter	Description	Type	Size	Default
type	Type of address.	option	-	ip
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
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		
<i>active</i>		Server status active.		
<i>standby</i>		Server status standby.		
<i>disable</i>		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 health check monitor continues to monitor and unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable per server health check.		
	<i>enable</i>	Enable per server health check.		
	<i>vip</i>	Use health check defined in VIP.		
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
max-connections	Max number of active connections that can be directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
	Option	Description		
cipher	Cipher suite name.	option	-	
	<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.		

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

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

Parameter	Description	Type	Size	Default
Option	Description			
<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.			
<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.			

Parameter	Description	Type	Size	Default
Option	Description			
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.			
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.			
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.			
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.			
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.			
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.			
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			
<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.			
<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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	-	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 ssl-server-cipher-suites

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

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

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

Parameter	Description	Type	Size	Default
Option	Description			
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.			
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.			
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.			
<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
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.		
	<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
	Option	Description		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		

Parameter	Description	Type	Size	Default
Option	Description			
<i>tls-1.2</i>	TLS 1.2.			
<i>tls-1.3</i>	TLS 1.3.			

config firewall vip6

Configure virtual IP for IPv6.

```
config firewall vip6
    Description: Configure virtual IP for IPv6.
    edit <name>
        set id {integer}
        set uuid {uuid}
        set comment {var-string}
        set type [static-nat|server-load-balance|...]
        set src-filter <rangel1>, <range2>, ...
        set extip {user}
        set mappedip {user}
        set nat-source-vip [disable|enable]
        set arp-reply [disable|enable]
        set portforward [disable|enable]
        set protocol [tcp|udp|...]
        set extport {user}
        set mappedport {user}
        set color {integer}
        set ldb-method [static|round-robin|...]
        set server-type [http|https|...]
        set http-redirect [enable|disable]
        set persistence [none|http-cookie|...]
        set nat66 [disable|enable]
        set nat64 [disable|enable]
        set add-nat64-route [disable|enable]
        config realservers
            Description: Select the real servers that this server load balancing VIP will
                        distribute traffic to.
            edit <id>
                set ip {user}
                set port {integer}
                set status [active|standby|...]
                set weight {integer}
                set holddown-interval {integer}
                set healthcheck [disable|enable|...]
                set http-host {string}
                set max-connections {integer}
                set monitor <name1>, <name2>, ...
                set client-ip {user}
            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-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 {string}
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-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-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 monitor <name1>, <name2>, ...
set max-embryonic-connections {integer}

```

```

set embedded-ipv4-address [disable|enable]
set ipv4-mappedip {user}
set ipv4-mappedport {user}
next
end

```

config firewall vip6

Parameter	Description	Type	Size	Default						
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 a static NAT server load balance VIP or access proxy.	option	-	static-nat						
Option										
<table border="1"> <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>					<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.	<i>access-proxy</i>	Access proxy.
<i>static-nat</i>	Static NAT.									
<i>server-load-balance</i>	Server load balance.									
<i>access-proxy</i>	Access proxy.									
src-filter <range>	Source IP6 filter (x:x:x:x:x:x/x). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79							
extip	IPv6 address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified							
mappedip	Mapped IPv6 address range in the format startIP-endIP.	user	Not Specified							
nat-source-vip	Enable to perform SNAT on traffic from mappedip to the extip for all egress interfaces.	option	-	disable						
Option										
<table border="1"> <tr> <td><i>disable</i></td><td>Disable nat-source-vip.</td></tr> <tr> <td><i>enable</i></td><td>Perform SNAT on traffic from mappedip to the extip for all egress interfaces.</td></tr> </table>					<i>disable</i>	Disable nat-source-vip.	<i>enable</i>	Perform SNAT on traffic from mappedip to the extip for all egress interfaces.		
<i>disable</i>	Disable nat-source-vip.									
<i>enable</i>	Perform SNAT on traffic from mappedip to the extip for all egress interfaces.									

Parameter	Description	Type	Size	Default
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable ARP reply.		
	<i>enable</i>	Enable ARP reply.		
portforward	Enable port forwarding.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable port forward.		
	<i>enable</i>	Enable/disable port forwarding.		
protocol	Protocol to use when forwarding packets.	option	-	tcp
	Option	Description		
	<i>tcp</i>	TCP.		
	<i>udp</i>	UDP.		
	<i>sctp</i>	SCTP.		
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	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute sessions based on source IP.		
	<i>round-robin</i>	Distribute sessions based round robin order.		
	<i>weighted</i>	Distribute sessions based on weight.		
	<i>least-session</i>	Sends new sessions to the server with the lowest session count.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.		
	<i>first-alive</i>	Distribute sessions to the first server that is alive.		
	<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.		
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-	
	Option	Description		
	<i>http</i>	HTTP.		
	<i>https</i>	HTTPS.		
	<i>imaps</i>	IMAPS.		
	<i>pop3s</i>	POP3S.		
	<i>smt�ps</i>	SMTPS.		
	<i>ssl</i>	SSL.		
	<i>tcp</i>	TCP.		
	<i>udp</i>	UDP.		
	<i>ip</i>	IP.		
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-	disable
	Option	Description		
	<i>enable</i>	Enable redirection of HTTP to HTTPS.		
	<i>disable</i>	Disable redirection of HTTP to HTTPS.		
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>http-cookie</i>	HTTP cookie.		
	<i>ssl-session-id</i>	SSL session ID.		
nat66	Enable/disable DNAT66.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable DNAT66.		
	<i>enable</i>	Enable DNAT66.		
nat64	Enable/disable DNAT64.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable DNAT64.		
	<i>enable</i>	Enable DNAT64.		
add-nat64-route	Enable/disable adding NAT64 route.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable adding NAT64 route.		
	<i>enable</i>	Enable adding NAT64 route.		
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookie-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

Parameter	Description	Type	Size	Default
http-cookie-share	Control sharing of cookies across virtual servers. same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option	Description		
	<i>disable</i>	Only allow HTTP cookie to match this virtual server.		
	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.		
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.		
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HTTP session multiplexing.		
	<i>disable</i>	Disable HTTP session multiplexing.		
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable adding HTTP header.		
	<i>disable</i>	Disable adding HTTP header.		
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35	
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Outlook Web Access support.		
	<i>enable</i>	Enable Outlook Web Access support.		

Parameter	Description	Type	Size	Default
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.		
	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.		
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.		
	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.		
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half
	Option	Description		
	<i>half</i>	Client to FortiGate SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		
ssl-certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35	
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 SSL sessions according to encryption strength.	option	-	high

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	Use AES.		
	<i>medium</i>	Use AES, 3DES, or RC4.		
	<i>low</i>	Use AES, 3DES, RC4, or DES.		
	<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.		
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client
	Option	Description		
	<i>high</i>	Use AES.		
	<i>medium</i>	Use AES, 3DES, or RC4.		
	<i>low</i>	Use AES, 3DES, RC4, or DES.		
	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.		
	<i>client</i>	Use the same encryption algorithms for client and server sessions.		
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
	Option	Description		
	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.		
	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.		
	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.		
ssl-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.		

Parameter	Description	Type	Size	Default														
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3														
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
Option	Description																	
<i>ssl-3.0</i>	SSL 3.0.																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
<i>client</i>	Use same value as client configuration.																	
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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-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														

Parameter	Description	Type	Size	Default
	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
	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
	Option	Description		
	<i>allow</i>	Allow a SSL client to renegotiate.		
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.		
	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.		
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both
	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 FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000

Parameter	Description	Type	Size	Default
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-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both
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 FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable
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
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
	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 minutes the web browser should keep HPKP.	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
	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
	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 honour 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.		
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000
embedded-ipv4-address	Enable/disable embedded IPv4 address.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable embedded IPv4 address.		
	<i>enable</i>	Enable embedded IPv4 address.		
ipv4-mappedip	Start-mapped-IPv4-address [-end mapped-IPv4-address].	user	Not Specified	
ipv4-mappedport	IPv4 port number range on the destination network to which the external port number range is mapped.	user	Not Specified	

config realservers

Parameter	Description	Type	Size	Default
ip	IP address of the real server.	user	Not Specified	
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		
	<i>active</i>	Server status active.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>standby</i>	Server status standby.		
	<i>disable</i>	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 health check monitor continues to monitor an unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip
	Option	Description		
	<i>disable</i>	Disable per server health check.		
	<i>enable</i>	Enable per server health check.		
	<i>vip</i>	Use health check defined in VIP.		
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
max-connections	Max number of active connections that can directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	

Parameter	Description	Type	Size	Default
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.			
<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.			
<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.			

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

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

Parameter	Description	Type	Size	Default
Option	Description			
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.			
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.			
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.			
<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
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.		
	<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
	Option	Description		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		

Parameter	Description	Type	Size	Default
	Option	Description		
<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
	Option	Description		
cipher	Cipher suite name.	option	-	
<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.			
<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.			

Parameter	Description	Type	Size	Default
Option	Description			
<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.			
<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.			

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

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

Parameter	Description	Type	Size	Default
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			
<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.			
<i>TLS-RSA- WITH-DES- CBC-SHA</i>	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 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
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 .	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79	

config firewall vipgrp6

Configure IPv6 virtual IP groups.

```
config firewall vipgrp6
  Description: Configure IPv6 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
  next
end
```

config firewall vipgrp6

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
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). IPv6 VIP name.	string	Maximum length: 79	

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
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 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
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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

config firewall ssh setting

SSH proxy settings.

```
config firewall ssh setting
  Description: SSH proxy settings.
  set caname {string}
  set 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	

Parameter	Description	Type	Size	Default
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 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
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
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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	Option	Description		
	256	The NID is ecdsa-sha2-nistp256.		
	384	The NID is ecdsa-sha2-nistp384.		
	521	The NID is ecdsa-sha2-nistp521.		
usage	Usage for this public key.	option	-	transparent-proxy
	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 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 {string}
    set host {string}
```

```

        set host-type [sub-string|wildcard]
    next
end

```

config firewall access-proxy-virtual-host

Parameter	Description	Type	Size	Default
ssl-certificate	SSL certificate for this host.	string	Maximum length: 35	
host	The host name.	string	Maximum length: 79	
host-type	Type of host pattern.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		

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

Parameter	Description	Type	Size	Default
	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
critical	Critical option.	option	-	no
	Option	Description		
	<i>no</i>	Certificate extension, server ignores the unsupported certificate extension.		
	<i>yes</i>	Critical option, server refuses to authorize if it cannnot recognize the critical option.		
type	Type of certificate extension.	option	-	fixed
	Option	Description		
	<i>fixed</i>	Fixed certificate extension entry.		
	<i>user</i>	Certificate extension entry filled with authenticated username.		
data	Data of certificate extension.	string	Maximum length: 127	

config firewall access-proxy

Configure IPv4 access proxy.

```
config firewall access-proxy
  Description: Configure IPv4 access proxy.
  edit <name>
    set vip {string}
    set client-cert [disable|enable]
    set empty-cert-action [accept|block]
    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|...]
        config realservers
```

```

Description: Select the real servers that this Access Proxy will distribute
            traffic to.
edit <id>
    set address {string}
    set ip {ipv4-address-any}
    set port {integer}
    set mappedport {user}
    set status [active|standby|...]
    set type [tcp-forwarding|ssh]
    set weight {integer}
    set http-host {string}
    set health-check [disable|enable]
    set health-check-proto [ping|http|...]
    set hold-down-interval [enable|disable]
    set ssh-client-cert {string}
    set ssh-host-key-validation [disable|enable]
    set ssh-host-key <name1>, <name2>, ...
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 saml-server {string}
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|...]
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|...]
        config realservers
            Description: Select the real servers that this Access Proxy will distribute
                        traffic to.
            edit <id>
                set address {string}
                set ip {ipv6-address}
                set port {integer}
                set mappedport {user}

```

```

        set status [active|standby|...]
        set type [tcp-forwarding|ssh]
        set weight {integer}
        set http-host {string}
        set health-check [disable|enable]
        set health-check-proto [ping|http|...]
        set holddown-interval [enable|disable]
        set ssh-client-cert {string}
        set ssh-host-key-validation [disable|enable]
        set ssh-host-key <name1>, <name2>, ...
    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 saml-server {string}
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|...]
next
end
next
end

```

config firewall access-proxy

Parameter	Description	Type	Size	Default
vip	Virtual IP name.	string	Maximum length: 79	
client-cert	Enable/disable to request client certificate.	option	-	disable
Option		Description		
		disable Disable client certificate request.		
		enable Enable client certificate request.		
empty-cert-action	Action of an empty client certificate.	option	-	block

Parameter	Description	Type	Size	Default
	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.		

config api-gateway

Parameter	Description	Type	Size	Default
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option	Description		
	<i>http</i>	HTTP		
	<i>https</i>	HTTPS		
	<i>tcp-forwarding</i>	TCP-FORWARDING		
	<i>samlsp</i>	SAML-SP		
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		
	<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
	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.		

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
	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 host field in HTTP (use http-cookie-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. 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

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	
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
	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
Option				
<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 realservers

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	::
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
Option				
	<i>active</i>			
	<i>standby</i>			
	<i>disable</i>			
type	TCP forwarding server type.	option	-	tcp-forwarding
Option				
	<i>tcp-forwarding</i>			
	<i>ssh</i>			

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
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.		
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	

config ssl-cipher-suites

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

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

Parameter	Description	Type	Size	Default
Option	Description			
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.			
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.			
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.			
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.			
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.			
<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
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.		
	<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 api-gateway6

Parameter	Description	Type	Size	Default
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option	Description		
	<i>http</i>	HTTP		
	<i>https</i>	HTTPS		
	<i>tcp-forwarding</i>	TCP-FORWARDING		
	<i>samlsp</i>	SAML-SP		
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		
	<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
	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.		
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.		

Parameter	Description	Type	Size	Default
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookie-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. <i>same-ip</i> 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	

Parameter	Description	Type	Size	Default
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048
	Option	Description		
	768	768-bit Diffie-Hellman prime.		
	1024	1024-bit Diffie-Hellman prime.		
	1536	1536-bit Diffie-Hellman prime.		
	2048	2048-bit Diffie-Hellman prime.		
	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
	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
	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
	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.		

config realservers

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	::
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
type	TCP forwarding server type.	option	-	tcp-forwarding
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
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
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
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
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

config firewall access-proxy6

Configure IPv6 access proxy.

```
config firewall access-proxy6
    Description: Configure IPv6 access proxy.
    edit <name>
        set vip {string}
        set client-cert [disable|enable]
        set empty-cert-action [accept|block]
        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|...]
                config realservers
                    Description: Select the real servers that this Access Proxy will distribute
                                traffic to.
                    edit <id>
                        set address {string}
                        set ip {ipv4-address-any}
                        set port {integer}
                        set mappedport {user}
                        set status [active|standby|...]
                        set type [tcp-forwarding|ssh]
                        set weight {integer}
                        set http-host {string}
                        set health-check [disable|enable]
                        set health-check-proto [ping|http|...]
                        set holddown-interval [enable|disable]
                        set ssh-client-cert {string}
                        set ssh-host-key-validation [disable|enable]
                        set ssh-host-key <name1>, <name2>, ...
                    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 saml-server {string}
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|...]
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|...]
    config realservers
        Description: Select the real servers that this Access Proxy will distribute
                    traffic to.
        edit <id>
            set address {string}
            set ip {ipv6-address}
            set port {integer}
            set mappedport {user}
            set status [active|standby|...]
            set type [tcp-forwarding|ssh]
            set weight {integer}
            set http-host {string}
            set health-check [disable|enable]
            set health-check-proto [ping|http|...]
            set holddown-interval [enable|disable]
            set ssh-client-cert {string}
            set ssh-host-key-validation [disable|enable]
            set ssh-host-key <name1>, <name2>, ...
        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 saml-server {string}
    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|...]
next
end
next
end

```

config firewall access-proxy6

Parameter	Description	Type	Size	Default
vip	Virtual IP name.	string	Maximum length: 79	
client-cert	Enable/disable to request client certificate.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable client certificate request.		
	<i>enable</i>	Enable client certificate request.		
empty-cert-action	Action of an empty client certificate.	option	-	block
	Option	Description		
	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.		
	<i>block</i>	Block the SSL handshake if the client certificate is empty.		

config api-gateway

Parameter	Description	Type	Size	Default
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option	Description		
	<i>http</i>	HTTP		
	<i>https</i>	HTTPS		
	<i>tcp-forwarding</i>	TCP-FORWARDING		
	<i>samlsp</i>	SAML-SP		

Parameter	Description	Type	Size	Default												
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.															
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>http-cookie</i></td><td>HTTP cookie.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cookie-domain setting).</td></tr> <tr> <td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookie-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-cookie-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													

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. 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	
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.		

Parameter	Description	Type	Size	Default
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
	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
	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 realservers

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	::
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443

Parameter	Description	Type	Size	Default								
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>tcp-forwarding</i></td><td>TCP forwarding.</td></tr> <tr> <td><i>ssh</i></td><td>SSH.</td></tr> </tbody> </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.											
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											

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
Option				
enable				
disable				
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				
disable				
enable				
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	
Option				
TLS-AES-128-GCM-SHA256				
TLS-AES-256-GCM-SHA384				
TLS-CHACHA20-POLY1305-SHA256				
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256				

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

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

Parameter	Description	Type	Size	Default
Option	Description			
<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.			
<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.			

Parameter	Description	Type	Size	Default
Option	Description			
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.			
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.			
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.			
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.			
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.			
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.			
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			
<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.			
<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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 1.1 tls-1.2 tls-1.3
	Option	Description		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config api-gateway6

Parameter	Description	Type	Size	Default
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option	Description		
	<i>http</i>	HTTP		
	<i>https</i>	HTTPS		
	<i>tcp-forwarding</i>	TCP-FORWARDING		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>samlsp</i>	SAML-SP		
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		
	<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
	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.		
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 host field in HTTP (use http-cookie-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 API Gateway. 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	
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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	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
	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
	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
	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.		

config realservers

Parameter	Description	Type	Size	Default
address	Address or address group of the real server.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
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
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
type	TCP forwarding server type.	option	-	tcp-forwarding
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
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
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
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
cipher	Cipher suite name.	option	-	

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

config firewall ipmacbinding setting

Configure IP to MAC binding settings.

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

config firewall ipmacbinding setting

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

config firewall ipmacbinding table

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

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

config firewall ipmacbinding table

Parameter	Description	Type	Size	Default
ip	IPv4 address portion of the pair (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
mac	MAC address portion of the pair (format: xx:xx:xx:xx:xx:xx in hexadecimal).	mac-address	Not Specified	00:00:00:00:00:00
name	Name of the pair .	string	Maximum length: 35	noname
status	Enable/disable this IP-mac binding pair.	option	-	disable

Option	Description
enable	Enable this IP-mac binding pair.
disable	Disable this IP-mac binding pair.

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 http
      Description: Configure HTTP protocol options.
      set ports {integer}
      set status [enable|disable]
      set inspect-all [enable|disable]
      set proxy-after-tcp-handshake [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 switching-protocols [bypass|block]
set unknown-http-version [reject|tunnel|...]
set tunnel-non-http [enable|disable]
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 block-page-status-code {integer}
set retry-count {integer}
set tcp-window-type [system|static|...]
set tcp-window-minimum {integer}
set tcp-window-maximum {integer}
set tcp-window-size {integer}
set ssl-offloaded [no|yes]
end
config ftp
    Description: Configure FTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [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 [system|static|...]
    set tcp-window-minimum {integer}
    set tcp-window-maximum {integer}
    set tcp-window-size {integer}
    set ssl-offloaded [no|yes]
end
config imap
    Description: Configure IMAP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [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 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 inspect-all [enable|disable]
    set proxy-after-tcp-handshake [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 inspect-all [enable|disable]
    set proxy-after-tcp-handshake [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 inspect-all [enable|disable]
    set proxy-after-tcp-handshake [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 [system|static|...]
    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 [system|static|...]
        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
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

Parameter	Description	Type	Size	Default
	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
	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
	Option	Description		
	<i>enable</i>	Enable inspection of RPC over HTTP.		
	<i>disable</i>	Disable inspection of RPC over HTTP.		

config http

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	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.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Parameter	Description	Type	Size	Default
	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/email.		
	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.		
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1
range-block	Enable/disable blocking of partial downloads.	option	-	disable
	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	-	

Parameter	Description	Type	Size	Default
	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>	Guoja 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.		
	<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
	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

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.		
	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.		
	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.		
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	-	disable
	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.		
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12

Parameter	Description	Type	Size	Default
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned .	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.		
block-page-status-code	Code number returned for blocked HTTP pages .	integer	Minimum value: 100 Maximum value: 599	403
retry-count	Number of attempts to retry HTTP connection .	integer	Minimum value: 0 Maximum value: 100	0
tcp-window-type	TCP window type to use for this protocol.	option	-	system
Option		Description		
		<i>system</i> Use system default TCP window size for this protocol (default).		
		<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: 33554432	8388608

Parameter	Description	Type	Size	Default
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	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 FortiGate when deep-inspection is enabled.		
<i>yes</i>		SSL decryption and encryption performed by an external device.		

** Values may differ between models.

config ftp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	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.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
Option		Description		
<i>enable</i>		Enable setting.		
<i>disable</i>		Disable setting.		
options	One or more options that can be applied to the session.	option	-	
Option		Description		
<i>clientcomfort</i>		Prevent client timeout.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>oversize</i>	Block oversized file/email.		
	<i>splice</i>	Enable splice mode.		
	<i>bypass-rest-command</i>	Bypass REST command.		
	<i>bypass-mode-command</i>	Bypass MODE command.		
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned .	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	-	system
	Option	Description		
	system	Use system default TCP window size for this protocol (default).		
	static	Manually specify TCP window size.		
	dynamic	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.		
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: 33554432	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option	Description		
	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.		
	yes	SSL decryption and encryption performed by an external device.		

** Values may differ between models.

config imap

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	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.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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.		
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 file/email.		
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12

Parameter	Description	Type	Size	Default						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr> <tr> <td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr> </tbody> </table>					Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									

** Values may differ between models.

config map

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>fragmail</i></td><td>Pass fragmented email.</td></tr> <tr> <td><i>oversize</i></td><td>Block oversized file/email.</td></tr> </tbody> </table>					Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									

Parameter	Description	Type	Size	Default						
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

** Values may differ between models.

config pop3

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>fragmail</i></td><td>Pass fragmented email.</td></tr> <tr> <td><i>oversize</i></td><td>Block oversized file/email.</td></tr> </tbody> </table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized file/email.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						

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

** Values may differ between models.

config smtp

Parameter	Description		Type	Size	Default
	Option	Description			
ports	Ports to scan for content .		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.			
inspect-all	Enable/disable the inspection of all ports for the protocol.		option	-	disable
	Option	Description			
	<i>enable</i>	Enable setting.			
	<i>disable</i>	Disable setting.			
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.			
options	One or more options that can be applied to the session.		option	-	
	Option	Description			
	<i>fragmail</i>	Pass fragmented email.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>oversize</i>	Block oversized file/email.		
	<i>splice</i>	Enable splice mode.		
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	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
	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 FortiGate when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

** Values may differ between models.

config nntp

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>oversize</i></td><td>Block oversized file/email.</td></tr> <tr> <td><i>splice</i></td><td>Enable splice mode.</td></tr> </tbody> </table>	Option	Description	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.			
Option	Description									
<i>oversize</i>	Block oversized file/email.									
<i>splice</i>	Enable splice mode.									
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10						

Parameter	Description	Type	Size	Default
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	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.		

** Values may differ between models.

config ssh

Parameter	Description	Type	Size	Default
options	One or more options that can be applied to the session.	option	-	
Option		Description		
		<i>oversize</i> Block oversized file/email.		
		<i>clientcomfort</i> Prevent client timeout.		
		<i>servercomfort</i> Prevent server timeout.		
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data .	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10

Parameter	Description	Type	Size	Default								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100	12								
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned .	integer	Minimum value: 0 Maximum value: 4294967295	0								
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					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	-	system								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>system</i></td><td>Use system default TCP window size for this protocol (default).</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> </tbody> </table>					Option	Description	<i>system</i>	Use system default TCP window size for this protocol (default).	<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>system</i>	Use system default TCP window size for this protocol (default).											
<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: 33554432	8388608								

Parameter	Description	Type	Size	Default
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	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 FortiGate when deep-inspection is enabled.		
		<i>yes</i> SSL decryption and encryption performed by an external device.		

** Values may differ between models.

config dns

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	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.		

config cifs

Parameter	Description	Type	Size	Default
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	Option	Description		
	<i>oversize</i>	Block oversized file/email.		
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 383 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 383 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	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	-	system
	Option	Description		
	<i>system</i>	Use system default TCP window size for this protocol (default).		
	<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.		

Parameter	Description	Type	Size	Default
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: 33554432	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	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	

** Values may differ between models.

config server-keytab

Parameter	Description	Type	Size	Default
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	

config mail-signature

Parameter	Description	Type	Size	Default
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiGate.	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 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]
    end
    config https
      Description: Configure HTTPS options.
      set ports {integer}
      set status [disable|certificate-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|...]
```

```

        set cert-probe-failure [allow|block]
    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|...]
    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 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
set allowlist [enable|disable]
set block-blocklisted-certificates [disable|enable]
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}
    next
end
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-anomalies-log [disable|enable]
set ssl-exemptions-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
comment	Optional comments.	var-string	Maximum length: 255	
allowlist	Enable/disable exempting servers by FortiGuard allowlist.	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blocklist.	option	-	enable
Option		Description		
		<i>disable</i> Disable FortiGuard certificate blocklist.		
		<i>enable</i> Enable FortiGuard certificate blocklist.		
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

Parameter	Description	Type	Size	Default
	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	Fortinet_CA_SSL
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted
server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 35	
ssl-anomalies-log	Enable/disable logging SSL anomalies.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging SSL anomalies.		
	<i>enable</i>	Enable logging SSL anomalies.		
ssl-exemptions-log	Enable/disable logging SSL exemptions.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging SSL exemptions.		
	<i>enable</i>	Enable logging SSL exemptions.		
ssl-negotiation-log	Enable/disable logging SSL negotiation.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging SSL negotiation.		
	<i>enable</i>	Enable logging SSL negotiation.		
ssl-server-cert-log	Enable/disable logging of server certificate information.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
		<i>disable</i> Disable logging server certificate.		
		<i>enable</i> Enable logging server certificate.		
ssl-handshake-log	Enable/disable logging of TLS handshakes.	option	-	disable
	Option	Description		
		<i>disable</i> Disable logging TLS handshakes.		
		<i>enable</i> Enable logging 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.		
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable
	Option	Description		
		<i>enable</i> Enable inspection of MAPI over HTTPS.		
		<i>disable</i> Disable inspection of MAPI over HTTPS.		
supported-alpn	Configure ALPN option.	option	-	all
	Option	Description		
		<i>http1-1</i> Enable ALPN of HTTP1.1.		
		<i>http2</i> Enable ALPN of HTTP2.		
		<i>all</i> Enable ALPN of HTTP1.1 and HTTP2.		
		<i>none</i> Do not use ALPN.		

config ssl

Parameter	Description	Type	Size	Default
inspect-all	Level of SSL inspection.	option	-	disable

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow
	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.		
	<i>inspect</i>	Inspect 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

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.		
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
	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

Parameter	Description	Type	Size	Default
	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.		

config https

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	Option	Description		
	<i>disable</i>	Disable.		
	<i>certificate-inspection</i>	Inspect SSL handshake only.		
	<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.		

Parameter	Description	Type	Size	Default
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.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow
	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.		
	<i>inspect</i>	Inspect 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

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.		
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
	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.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<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.			

config ftps

Parameter	Description	Type	Size	Default	
ports	Ports to use for scanning .	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.			
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow	
	Option	Description			
	<i>allow</i>	Bypass the session when the version is not supported.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the session when the version is not supported.		
	<i>inspect</i>	Inspect 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.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
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 imaps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535	

Parameter	Description	Type	Size	Default
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.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow
	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.		
	<i>inspect</i>	Inspect 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 pop3s

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	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.		

Parameter	Description	Type	Size	Default
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.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow
	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.		
	<i>inspect</i>	Inspect 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

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.		
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
	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 .	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> <tr> <td><i>inspect</i></td><td>Inspect the session when the version is not supported.</td></tr> </tbody> </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.	<i>inspect</i>	Inspect 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.											
<i>inspect</i>	Inspect 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 ssh

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning .	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.		

Parameter	Description	Type	Size	Default						
inspect-all	Level of SSL inspection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>bypass</i></td><td>Bypass the session.</td></tr> <tr> <td><i>block</i></td><td>Block the session.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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

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	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	allow
	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.		
	<i>inspect</i>	Inspect 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.		

Parameter	Description	Type	Size	Default
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
	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
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 ssl-exempt

Parameter	Description	Type	Size	Default
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.		
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	

config ssl-server

Parameter	Description	Type	Size	Default								
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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
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								

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.		
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 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 webfilter-profile {string}
    set dnsfilter-profile {string}
    set emailfilter-profile {string}
    set dlp-sensor {string}
    set file-filter-profile {string}
    set ips-sensor {string}
    set application-list {string}
    set voip-profile {string}
    set sctp-filter-profile {string}
    set icap-profile {string}
    set cifs-profile {string}
    set videofilter-profile {string}
    set waf-profile {string}
    set ssh-filter-profile {string}
  next
end
```

config firewall profile-group

Parameter	Description	Type	Size	Default
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	
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	
dlp-sensor	Name of an existing DLP sensor.	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	
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35	
sctp-filter-profile	Name of an existing SCTP filter profile.	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	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	

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 {string}
    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
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
port	Server service port .	integer	Minimum value: 1 Maximum value: 65535	443
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full
Option		Description		
		<i>half</i> Client to FortiGate SSL.		
		<i>full</i> Client to FortiGate and FortiGate to Server SSL.		
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable
Option		Description		
		<i>enable</i> Add X-Forwarded-Proto header.		
		<i>disable</i> Do not add X-Forwarded-Proto header.		

Parameter	Description	Type	Size	Default
mapped-port	Mapped server service port .	integer	Minimum value: 1 Maximum value: 65535	80
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35	Fortinet_CA_SSL
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048
Option		Description		
		768 768-bit Diffie-Hellman prime.		
		1024 1024-bit Diffie-Hellman prime.		
		1536 1536-bit Diffie-Hellman prime.		
		2048 2048-bit Diffie-Hellman prime.		
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
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-client-renegotiation	Allow or block client renegotiation by server.	option	-	allow
Option		Description		
		allow Allow a SSL client to renegotiate.		
		deny Abort any SSL connection that attempts to renegotiate.		
		secure Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.		
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1
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.		

Parameter	Description	Type	Size	Default
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.2
	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 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
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 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
comments	Comments.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
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 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}
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	

config firewall security-policy

Configure NGFW IPv4/IPv6 application policies.

```
config firewall security-policy
  Description: Configure NGFW IPv4/IPv6 application policies.
  edit <policyid>
    set uuid {uuid}
```

```
set name {string}
set comments {var-string}
set srcintf <name1>, <name2>, ...
set dstintf <name1>, <name2>, ...
set srcaddr <name1>, <name2>, ...
set dstaddr <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set dstaddr6 <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set dstaddr-negate [enable|disable]
set internet-service [enable|disable]
set internet-service-name <name1>, <name2>, ...
set internet-service-negate [enable|disable]
set internet-service-group <name1>, <name2>, ...
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-src [enable|disable]
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-negate [enable|disable]
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set enforce-default-app-port [enable|disable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set action [accept|deny]
set send-deny-packet [disable|enable]
set schedule {string}
set status [enable|disable]
set logtraffic [all|utm|...]
set learning-mode [enable|disable]
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set voip-profile {string}
set sctp-filter-profile {string}
set icap-profile {string}
set cifs-profile {string}
set videofilter-profile {string}
set ssh-filter-profile {string}
set application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set url-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set fssouser-groups <name1>, <name2>, ...
next
```

end

config firewall security-policy

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-000000000000
name	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
srcaddr <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination IPv4 address name and address group names. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79	
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable
Option	Description			
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
dstaddr-negate	When enabled dstaddr/dstaddr6 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.		
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable
	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-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-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	
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of Internet Services source in policy.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable use of Internet Services source in policy.		
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79	
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negated Internet Service source match.		
	<i>disable</i>	Disable negated Internet Service source match.		
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79	
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79	
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79	
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
service <name>	Service and service group names. Service name.	string	Maximum length: 79	
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable negated service match.		
	<i>disable</i>	Disable negated service match.		
action	Policy action (accept/deny).	option	-	deny
	Option	Description		
	<i>accept</i>	Allows session that match the firewall policy.		
	<i>deny</i>	Blocks sessions that match the firewall policy.		
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable deny-packet sending.		
	<i>enable</i>	Enable deny-packet sending.		
schedule	Schedule name.	string	Maximum length: 35	
status	Enable or disable this policy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm
	Option	Description		
	<i>all</i>	Log all sessions accepted or denied by this policy.		
	<i>utm</i>	Log traffic that has a security profile applied to it.		
	<i>disable</i>	Disable all logging for this policy.		
learning-mode	Enable to allow everything, but log all of the meaningful data for security information gathering. A learning report will be generated.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable learning mode.		
	<i>disable</i>	Disable learning mode.		

Parameter	Description	Type	Size	Default
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single
	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	
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	
dlp-sensor	Name of an existing DLP sensor.	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	
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35	
sctp-filter-profile	Name of an existing SCTP filter profile.	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	

Parameter	Description	Type	Size	Default
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
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	
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	Application group names. Application group names.	string	Maximum length: 79	
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79	
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79	
fssouser-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511	

config firewall policy

Configure IPv4/IPv6 policies.

```
config firewall policy
  Description: Configure IPv4/IPv6 policies.
  edit <policyid>
    set status [enable|disable]
    set name {string}
    set uuid {uuid}
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set action [accept|deny|...]
    set nat64 [enable|disable]
```

```
set nat46 [enable|disable]
set srcaddr <name1>, <name2>, ...
set dstaddr <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set dstaddr6 <name1>, <name2>, ...
set ztna-status [enable|disable]
set ztna-ems-tag <name1>, <name2>, ...
set ztna-geo-tag <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-service-custom-group <name1>, <name2>, ...
set internet-service-src [enable|disable]
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set reputation-minimum {integer}
set reputation-direction [source|destination]
set src-vendor-mac <id1>, <id2>, ...
set rtp-nat [disable|enable]
set rtp-addr <name1>, <name2>, ...
set send-deny-packet [disable|enable]
set firewall-session-dirty [check-all|check-new]
set schedule {string}
set schedule-timeout [enable|disable]
set service <name1>, <name2>, ...
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set anti-replay [enable|disable]
set tcp-session-without-syn [all|data-only|...]
set geoip-anycast [enable|disable]
set geoip-match [physical-location|registered-location]
set dynamic-shaping [enable|disable]
set passive-wan-health-measurement [enable|disable]
set utm-status [enable|disable]
set inspection-mode [proxy|flow]
set http-policy-redirect [enable|disable]
set ssh-policy-redirect [enable|disable]
set webproxy-profile {string}
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set voip-profile {string}
set sctp-filter-profile {string}
set icap-profile {string}
```

```
set cifs-profile {string}
set videofilter-profile {string}
set waf-profile {string}
set ssh-filter-profile {string}
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set auto-asic-offload [enable|disable]
set np-acceleration [enable|disable]
set webproxy-forward-server {string}
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set per-ip-shaper {string}
set nat [enable|disable]
set permit-any-host [enable|disable]
set permit-stun-host [enable|disable]
set fixedport [enable|disable]
set ippool [enable|disable]
set poolname <name1>, <name2>, ...
set poolname6 <name1>, <name2>, ...
set session-ttl {user}
set vlan-cos-fwd {integer}
set vlan-cos-rev {integer}
set inbound [enable|disable]
set outbound [enable|disable]
set natinbound [enable|disable]
set natoutbound [enable|disable]
set wccp [enable|disable]
set ntlm [enable|disable]
set ntlm-guest [enable|disable]
set ntlm-enabled-browsers <user-agent-string1>, <user-agent-string2>, ...
set fssso-agent-for-ntlm {string}
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set fssso-groups <name1>, <name2>, ...
set auth-path [enable|disable]
set disclaimer [enable|disable]
set email-collect [enable|disable]
set vpntunnel {string}
set natip {ipv4-classnet}
set match-vip [enable|disable]
set match-vip-only [enable|disable]
set diffserv-forward [enable|disable]
set diffserv-reverse [enable|disable]
set diffservcode-forward {user}
set diffservcode-rev {user}
set tcp-mss-sender {integer}
set tcp-mss-receiver {integer}
set comments {var-string}
set auth-cert {string}
set auth-redirect-addr {string}
set redirect-url {var-string}
set identity-based-route {string}
set block-notification [enable|disable]
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-service-src-negate [enable|disable]
set timeout-send-rst [enable|disable]
set captive-portal-exempt [enable|disable]
set decrypted-traffic-mirror {string}
set dsri [enable|disable]
set radius-mac-auth-bypass [enable|disable]
set delay-tcp-npu-session [enable|disable]
set vlan-filter {user}
set sgt-check [enable|disable]
set sgt <id1>, <id2>, ...
next
end

```

config firewall policy

Parameter	Description	Type	Size	Default
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
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
action	Policy action (accept/deny/ipsec).	option	-	deny
	Option	Description		
	<i>accept</i>	Allows session that match the firewall policy.		
	<i>deny</i>	Blocks sessions that match the firewall policy.		
	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.		
nat64	Enable/disable NAT64.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NAT64.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable NAT64.		
nat46	Enable/disable NAT46.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NAT46.		
	<i>disable</i>	Disable NAT46.		
srcaddr <name>	Source IPv4 address and address group names. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination IPv4 address and address group names. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79	
ztna-status	Enable/disable zero trust access.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable zero trust network access.		
	<i>disable</i>	Disable zero trust network access.		
ztna-ems-tag <name>	Source ztna-ems-tag names. Address name.	string	Maximum length: 79	
ztna-geo-tag <name>	Source ztna-geo-tag names. Address 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
	Option	Description		
	<i>enable</i>	Enable use of Internet Services in policy.		
	<i>disable</i>	Disable use of Internet Services in policy.		

Parameter	Description	Type	Size	Default
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-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79	
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of Internet Services source in policy.		
	<i>disable</i>	Disable use of Internet Services source in policy.		
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79	
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79	
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79	
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79	
reputation-minimum	Minimum Reputation to take action.	integer	Minimum value: 0 Maximum value: 4294967295	0
reputation-direction	Direction of the initial traffic for reputation to take effect.	option	-	destination
	Option	Description		
	<i>source</i>	Check reputation for source address.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>destination</i>	Check reputation for destination address.		
src-vendor-mac <id>	Vendor MAC source ID. Vendor MAC ID.	integer	Minimum value: 0 Maximum value: 4294967295	
rtp-nat	Enable Real Time Protocol (RTP) NAT.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable setting.		
	<i>enable</i>	Enable setting.		
rtp-addr <name>	Address names if this is an RTP NAT policy. Address name.	string	Maximum length: 79	
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable deny-packet sending.		
	<i>enable</i>	Enable deny-packet sending.		
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-	check-all
	Option	Description		
	<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.		
	<i>check-new</i>	Continue to allow sessions already accepted by this policy.		
schedule	Schedule name.	string	Maximum length: 35	
schedule-timeout	Enable to force current sessions to end when the schedule object times out. Disable allows them to end from inactivity.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable schedule timeout.		
	<i>disable</i>	Disable schedule timeout.		

Parameter	Description	Type	Size	Default								
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79									
tos	ToS (Type of Service) value used for comparison.	user	Not Specified									
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified									
tos-negate	Enable negated TOS match.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable TOS match negate.</td></tr> <tr> <td><i>disable</i></td><td>Disable TOS match negate.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable TOS match negate.	<i>disable</i>	Disable TOS match negate.		
Option	Description											
<i>enable</i>	Enable TOS match negate.											
<i>disable</i>	Disable TOS match negate.											
anti-replay	Enable/disable anti-replay check.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable anti-replay check.</td></tr> <tr> <td><i>disable</i></td><td>Disable anti-replay check.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable anti-replay check.	<i>disable</i>	Disable anti-replay check.		
Option	Description											
<i>enable</i>	Enable anti-replay check.											
<i>disable</i>	Disable anti-replay check.											
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>all</i></td><td>Enable TCP session without SYN.</td></tr> <tr> <td><i>data-only</i></td><td>Enable TCP session data only.</td></tr> <tr> <td><i>disable</i></td><td>Disable TCP session without SYN.</td></tr> </tbody> </table>				Option	Description	<i>all</i>	Enable TCP session without SYN.	<i>data-only</i>	Enable TCP session data only.	<i>disable</i>	Disable TCP session without SYN.
Option	Description											
<i>all</i>	Enable TCP session without SYN.											
<i>data-only</i>	Enable TCP session data only.											
<i>disable</i>	Disable TCP session without SYN.											
geoip-anycast	Enable/disable recognition of anycast IP addresses using the geography IP database.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable recognition of anycast IP addresses using the geography IP database.</td></tr> <tr> <td><i>disable</i></td><td>Disable recognition of anycast IP addresses using the geography IP database.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.	<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.		
Option	Description											
<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.											
<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.											
geoip-match	Match geography address based either on its physical location or registered location.	option	-	physical-location								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>physical-location</i>	Match geography address to its physical location using the geography IP database.		
	<i>registered-location</i>	Match geography address to its registered location using the geography IP database.		
dynamic-shaping	Enable/disable dynamic RADIUS defined traffic shaping.	option	-	disable
	<i>enable</i>	Enable dynamic RADIUS defined traffic shaping.		
	<i>disable</i>	Disable dynamic RADIUS defined traffic shaping.		
passive-wan-health-measurement	Enable/disable passive WAN health measurement. When enabled, auto-asic-offload is disabled.	option	-	disable
	<i>enable</i>	Enable Passive WAN health measurement.		
	<i>disable</i>	Disable Passive WAN health measurement.		
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-	flow
	<i>proxy</i>	Proxy based inspection.		
	<i>flow</i>	Flow based inspection.		
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-	disable
	<i>enable</i>	Enable HTTP(S) policy redirect.		
	<i>disable</i>	Disable HTTP(S) policy redirect.		

Parameter	Description	Type	Size	Default
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSH policy redirect.		
	<i>disable</i>	Disable SSH policy redirect.		
webproxy-profile	Webproxy profile name.	string	Maximum length: 63	
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single
	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	
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	
dlp-sensor	Name of an existing DLP sensor.	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	

Parameter	Description	Type	Size	Default								
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35									
sctp-filter-profile	Name of an existing SCTP filter profile.	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									
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35									
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>					Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
logtraffic-start	Record logs when a session starts.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
auto-asic-offload	Enable/disable policy traffic ASIC offloading.	option	-	enable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable auto ASIC offloading.</td></tr> <tr> <td><i>disable</i></td><td>Disable ASIC offloading.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.		
Option	Description											
<i>enable</i>	Enable auto ASIC offloading.											
<i>disable</i>	Disable ASIC offloading.											
np-acceleration*	Enable/disable UTM Network Processor acceleration.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable UTM Network Processor acceleration.		
	<i>disable</i>	Disable UTM Network Processor acceleration.		
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63	
traffic-shaper	Traffic shaper.	string	Maximum length: 35	
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35	
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35	
nat	Enable/disable source NAT.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-any-host	Accept UDP packets from any host.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-stun-host	Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ippool	Enable to use IP Pools for source NAT.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79	
poolname6 <name>	IPv6 pool names. IPv6 pool name.	string	Maximum length: 79	
session-ttl	TTL in seconds for sessions accepted by this policy.	user	Not Specified	
vlan-cos-fwd	VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255
vlan-cos-rev	VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
wccp	Enable/disable forwarding traffic matching this policy to a configured WCCP server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WCCP setting.		
	<i>disable</i>	Disable WCCP setting.		
ntlm	Enable/disable NTLM authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ntlm-guest	Enable/disable NTLM guest user access.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ntlm-enabled-browsers <user-agent-string>	HTTP-User-Agent value of supported browsers. User agent string.	string	Maximum length: 79	
fssso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35	
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	

Parameter	Description	Type	Size	Default
fssso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511	
auth-path	Enable/disable authentication-based routing.	option	-	disable
	Option	Description		
	enable	Enable authentication-based routing.		
	disable	Disable authentication-based routing.		
disclaimer	Enable/disable user authentication disclaimer.	option	-	disable
	Option	Description		
	enable	Enable user authentication disclaimer.		
	disable	Disable user authentication disclaimer.		
email-collect	Enable/disable email collection.	option	-	disable
	Option	Description		
	enable	Enable email collection.		
	disable	Disable email collection.		
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35	
natip	Policy-based IPsec VPN: source NAT IP address for outgoing traffic.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
match-vip	Enable to match packets that have had their destination addresses changed by a VIP.	option	-	disable
	Option	Description		
	enable	Match DNATed packet.		
	disable	Do not match DNATed packet.		
match-vip-only	Enable/disable matching of only those packets that have had their destination addresses changed by a VIP.	option	-	disable
	Option	Description		
	enable	Enable matching of only those packets that have had their destination addresses changed by a VIP.		
	disable	Disable matching of only those packets that have had their destination addresses changed by a VIP.		

Parameter	Description	Type	Size	Default
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting forward (original) traffic Diffserv.		
	<i>disable</i>	Disable setting forward (original) traffic Diffserv.		
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.		
	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.		
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified	
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified	
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535	0
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535	0
comments	Comment.	var-string	Maximum length: 1023	
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35	
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication.	string	Maximum length: 63	
redirect-url	URL users are directed to after seeing and accepting the disclaimer or authenticating.	var-string	Maximum length: 1023	
identity-based-route	Name of identity-based routing rule.	string	Maximum length: 35	
block-notification	Enable/disable block notification.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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/srcaddr6 specifies what the source address must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
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-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable negated Internet Service source match.		
	<i>disable</i>	Disable negated Internet Service source match.		
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sending of RST packet upon TCP session expiration.		
	<i>disable</i>	Disable sending of RST packet upon TCP session expiration.		
captive-portal-exempt	Enable to exempt some users from the captive portal.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable exemption of captive portal.		
	<i>disable</i>	Disable exemption of captive portal.		
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	
dsri	Enable DSRI to ignore HTTP server responses.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable MAC authentication bypass.		
	<i>disable</i>	Disable MAC authentication bypass.		
delay-tcp-npu-session	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.		
	<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.		
vlan-filter	Set VLAN filters.	user	Not Specified	
sgt-check	Enable/disable security group tags (SGT) check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SGT check.		
	<i>disable</i>	Disable SGT check.		
sgt <id>	Security group tags. Security group tag.	integer	Minimum value: 0 Maximum value: 4294967295	

* This parameter may not exist in some models.

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-name	Define the name for this class-id.	string	Maximum length: 35	

config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
```

```

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

```

config firewall shaping-policy

Parameter	Description	Type	Size	Default
name	Shaping policy name.	string	Maximum length: 35	
comment	Comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
status	Enable/disable this traffic shaping policy.	option	-	enable
	Option	Description		
	enable	Enable traffic shaping policy.		
	disable	Disable traffic shaping policy.		
ip-version	Apply this traffic shaping policy to IPv4 or IPv6 traffic.	option	-	4
	Option	Description		
	4	Use IPv4 addressing for Configuration Method.		
	6	Use IPv6 addressing for Configuration Method.		
srcaddr <name>	IPv4 source address and address group names. Address name.	string	Maximum length: 79	
dstaddr <name>	IPv4 destination address and address group names. Address name.	string	Maximum length: 79	
srcaddr6 <name>	IPv6 source address and address group names. Address name.	string	Maximum length: 79	
dstaddr6 <name>	IPv6 destination address and address group names. Address 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
	Option	Description		
	enable	Enable use of Internet Service in shaping-policy.		
	disable	Disable use of Internet Service in shaping-policy.		
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	

Parameter	Description	Type	Size	Default
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79	
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable
Option		Description		
		enable	Enable use of Internet Service source in shaping-policy.	
		disable	Disable use of Internet Service source in shaping-policy.	
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79	
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79	
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79	
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79	
service <name>	Service and service group names. Service name.	string	Maximum length: 79	
schedule	Schedule name.	string	Maximum length: 35	
users <name>	Apply this traffic shaping policy to individual users that have authenticated with the FortiGate. User name.	string	Maximum length: 79	
groups <name>	Apply this traffic shaping policy to user groups that have authenticated with the FortiGate. Group name.	string	Maximum length: 79	
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	

Parameter	Description	Type	Size	Default
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79	
url-category <id>	IDs of one or more FortiGuard Web Filtering categories that this shaper applies traffic shaping to. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
srcintf <name>	One or more incoming (ingress) interfaces. Interface name.	string	Maximum length: 79	
dstintf <name>	One or more outgoing (egress) interfaces. Interface name.	string	Maximum length: 79	
tos	ToS (Type of Service) value used for comparison.	user	Not Specified	
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified	
tos-negate	Enable negated TOS match.	option	-	disable
Option	Description			
enable	Enable TOS match negate.			
disable	Disable TOS match negate.			
traffic-shaper	Traffic shaper to apply to traffic forwarded by the firewall policy.	string	Maximum length: 35	
traffic-shaper-reverse	Traffic shaper to apply to response traffic received by the firewall policy.	string	Maximum length: 35	
per-ip-shaper	Per-IP traffic shaper to apply with this policy.	string	Maximum length: 35	
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
difftserv-forward	Enable to change packet's DiffServ values to the specified difftservcode-forward value.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting forward (original) traffic DiffServ.		
	<i>disable</i>	Disable setting forward (original) traffic DiffServ.		
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.		
	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.		
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified	
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified	

config firewall shaping-profile

Configure shaping profiles.

```
config firewall shaping-profile
  Description: Configure shaping profiles.
  edit <profile-name>
    set comment {var-string}
    set type [policing|queuing]
    set default-class-id {integer}
    config shaping-entries
      Description: Define shaping entries of this shaping profile.
      edit <id>
        set class-id {integer}
        set priority [top|critical|...]
        set guaranteed-bandwidth-percentage {integer}
        set maximum-bandwidth-percentage {integer}
        set limit {integer}
        set burst-in-msec {integer}
        set cburst-in-msec {integer}
        set red-probability {integer}
        set min {integer}
        set max {integer}
      next
    end
  next
end
```

config firewall shaping-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
type	Select shaping profile type: policing / queuing.	option	-	policing
Option		Description		
		<i>policing</i> Enable policing mode.		
		<i>queuing</i> Enable queuing mode.		
default-class-id	Default class ID to handle unclassified packets (including all local traffic).	integer	Minimum value: 0 Maximum value: 4294967295	0

config shaping-entries

Parameter	Description	Type	Size	Default
class-id	Class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
priority	Priority.	option	-	high
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-percentage	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100	0
maximum-bandwidth-percentage	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1

Parameter	Description	Type	Size	Default
limit	Hard limit on the real queue size in packets.	integer	Minimum value: 5 Maximum value: 10000	1000
burst-in-msec	Number of bytes that can be burst at maximum-bandwidth speed. Formula: burst = maximum-bandwidth*burst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
cburst-in-msec	Number of bytes that can be burst as fast as the interface can transmit. Formula: cburst = maximum-bandwidth*cburst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
red-probability	Maximum probability (in percentage) for RED marking.	integer	Minimum value: 0 Maximum value: 20	0
min	Average queue size in packets at which RED drop becomes a possibility.	integer	Minimum value: 3 Maximum value: 3000	83
max	Average queue size in packets at which RED drop probability is maximal.	integer	Minimum value: 3 Maximum value: 3000	250

config firewall local-in-policy

Configure user defined IPv4 local-in policies.

```
config firewall local-in-policy
  Description: Configure user defined IPv4 local-in policies.
  edit <policyid>
    set uuid {uuid}
    set ha-mgmt-intf-only [enable|disable]
    set intf {string}
    set srcaddr <name1>, <name2>, ...
    set srcaddr-negate [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set action {accept|deny}
    set service <name1>, <name2>, ...
    set service-negate [enable|disable]
    set schedule {string}
    set status {enable|disable}
    set comments {var-string}
  next
end
```

config firewall local-in-policy

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
ha-mgmt-intf-only	Enable/disable dedicating the HA management interface only for local-in policy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dedicating HA management interface only for local-in policy.		
	<i>disable</i>	Disable dedicating HA management interface only for local-in policy.		
intf	Incoming interface name from available options.	string	Maximum length: 35	
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79	
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79	
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
action	Action performed on traffic matching the policy .	option	-	deny
	Option	Description		
	<i>accept</i>	Allow traffic matching this policy.		
	<i>deny</i>	Deny or block traffic matching this policy.		
service <name>	Service object from available options. Service name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
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.		
schedule	Schedule object from available options.	string	Maximum length: 35	
status	Enable/disable this local-in policy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this local-in policy.		
	<i>disable</i>	Disable this local-in policy.		
comments	Comment.	var-string	Maximum length: 1023	

config firewall local-in-policy6

Configure user defined IPv6 local-in policies.

```
config firewall local-in-policy6
  Description: Configure user defined IPv6 local-in policies.
  edit <policyid>
    set uuid {uuid}
    set intf {string}
    set srcaddr <name1>, <name2>, ...
    set srcaddr-negate [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set action [accept|deny]
    set service <name1>, <name2>, ...
    set service-negate [enable|disable]
    set schedule {string}
    set status [enable|disable]
    set comments {var-string}
  next
end
```

config firewall local-in-policy6

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						
intf	Incoming interface name from available options.	string	Maximum length: 35							
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 <name>	Destination address object from available options. Address name.	string	Maximum length: 79							
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable destination address negate.</td></tr> <tr> <td><i>disable</i></td><td>Disable destination address negate.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable destination address negate.	<i>disable</i>	Disable destination address negate.
Option	Description									
<i>enable</i>	Enable destination address negate.									
<i>disable</i>	Disable destination address negate.									
action	Action performed on traffic matching the policy .	option	-	deny						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>accept</i></td><td>Allow local-in traffic matching this policy.</td></tr> <tr> <td><i>deny</i></td><td>Deny or block local-in traffic matching this policy.</td></tr> </tbody> </table>					Option	Description	<i>accept</i>	Allow local-in traffic matching this policy.	<i>deny</i>	Deny or block local-in traffic matching this policy.
Option	Description									
<i>accept</i>	Allow local-in traffic matching this policy.									
<i>deny</i>	Deny or block local-in traffic matching this policy.									
service <name>	Service object from available options. Separate names with a space. Service name.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable negated service match.</td></tr> <tr> <td><i>disable</i></td><td>Disable negated service match.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.
Option	Description									
<i>enable</i>	Enable negated service match.									
<i>disable</i>	Disable negated service match.									

Parameter	Description	Type	Size	Default
schedule	Schedule object from available options.	string	Maximum length: 35	
status	Enable/disable this local-in policy.	option	-	enable
	Option	Description		
	enable	Enable this local-in policy.		
	disable	Disable this local-in policy.		
comments	Comment.	var-string	Maximum length: 1023	

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
status	Enable/disable this TTL policy.	option	-	enable
	Option	Description		
	enable	Enable this TTL policy.		
	disable	Disable this TTL policy.		
action	Action to be performed on traffic matching this policy .	option	-	deny
	Option	Description		
	accept	Allow traffic matching this policy.		
	deny	Deny or block traffic matching this policy.		

Parameter	Description	Type	Size	Default
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 .	user	Not Specified	

config firewall proxy-policy

Configure proxy policies.

```
config firewall proxy-policy
  Description: Configure proxy policies.
  edit <policyid>
    set uuid {uuid}
    set name {string}
    set proxy [explicit-web|transparent-web|...]
    set access-proxy <name1>, <name2>, ...
    set access-proxy6 <name1>, <name2>, ...
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set poolname <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set ztna-ems-tag <name1>, <name2>, ...
    set device-ownership [enable|disable]
    set internet-service [enable|disable]
    set internet-service-negate [enable|disable]
    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 service <name1>, <name2>, ...
    set srcaddr-negate [enable|disable]
    set dstaddr-negate [enable|disable]
    set service-negate [enable|disable]
    set action [accept|deny|...]
    set status [enable|disable]
    set schedule {string}
    set logtraffic [all|utm|...]
    set session-ttl {integer}
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
```

```

set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set http-tunnel-auth [enable|disable]
set ssh-policy-redirect [enable|disable]
set webproxy-forward-server {string}
set webproxy-profile {string}
set transparent [enable|disable]
set disclaimer [disable|domain|...]
set utm-status [enable|disable]
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set webfilter-profile {string}
set emailfilter-profile {string}
set dlp-sensor {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set voip-profile {string}
set sctp-filter-profile {string}
set icap-profile {string}
set cifs-profile {string}
set videofilter-profile {string}
set waf-profile {string}
set ssh-filter-profile {string}
set replacemsg-override-group {string}
set logtraffic-start [enable|disable]
set comments {var-string}
set redirect-url {var-string}
set decrypted-traffic-mirror {string}
next
end

```

config firewall proxy-policy

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	Policy name.	string	Maximum length: 35	
proxy	Type of explicit proxy.	option	-	
Option	Description			
<i>explicit-web</i>	Explicit Web Proxy			
<i>transparent-web</i>	Transparent Web Proxy			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ftp</i>	Explicit FTP Proxy		
	<i>ssh</i>	SSH Proxy		
	<i>ssh-tunnel</i>	SSH Tunnel		
	<i>access-proxy</i>	Access Proxy		
access-proxy <name>	IPv4 access proxy. Access Proxy name.	string	Maximum length: 79	
access-proxy6 <name>	IPv6 access proxy. Access proxy name.	string	Maximum length: 79	
srcintf <name>	Source interface names. Interface name.	string	Maximum length: 79	
dstintf <name>	Destination interface names. Interface name.	string	Maximum length: 79	
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79	
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79	
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79	
ztna-ems-tag <name>	ZTNA EMS Tag names. EMS Tag name.	string	Maximum length: 79	
device-ownership	When enabled, the ownership enforcement will be done at policy level.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable device ownership.		
	<i>disable</i>	Disable device ownership.		
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of Internet Services in policy.		
	<i>disable</i>	Disable use of Internet Services in policy.		

Parameter	Description	Type	Size	Default
internet-service-negate	When enabled, Internet Services match against any internet service EXCEPT the selected Internet Service.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negated Internet Service match.		
	<i>disable</i>	Disable negated Internet Service match.		
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-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79	
service <name>	Name of service objects. Service name.	string	Maximum length: 79	
srcaddr-negate	When enabled, source addresses match against any address EXCEPT the specified source addresses.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable destination address negate.		
dstaddr-negate	When enabled, destination addresses match against any address EXCEPT the specified destination addresses.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable destination address negate.		

Parameter	Description	Type	Size	Default								
service-negate	When enabled, services match against any service EXCEPT the specified destination services.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable negated service match.</td></tr> <tr> <td><i>disable</i></td><td>Disable negated service match.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.					
Option	Description											
<i>enable</i>	Enable negated service match.											
<i>disable</i>	Disable negated service match.											
action	Accept or deny traffic matching the policy parameters.	option	-	deny								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>accept</i></td><td>Action accept.</td></tr> <tr> <td><i>deny</i></td><td>Action deny.</td></tr> <tr> <td><i>redirect</i></td><td>Action redirect.</td></tr> </tbody> </table>	Option	Description	<i>accept</i>	Action accept.	<i>deny</i>	Action deny.	<i>redirect</i>	Action redirect.			
Option	Description											
<i>accept</i>	Action accept.											
<i>deny</i>	Action deny.											
<i>redirect</i>	Action redirect.											
status	Enable/disable the active status of the policy.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
schedule	Name of schedule object.	string	Maximum length: 35									
logtraffic	Enable/disable logging traffic through the policy.	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>all</i></td><td>Log all sessions.</td></tr> <tr> <td><i>utm</i></td><td>UTM event and matched application traffic log.</td></tr> <tr> <td><i>disable</i></td><td>Disable traffic and application log.</td></tr> </tbody> </table>	Option	Description	<i>all</i>	Log all sessions.	<i>utm</i>	UTM event and matched application traffic log.	<i>disable</i>	Disable traffic and application log.			
Option	Description											
<i>all</i>	Log all sessions.											
<i>utm</i>	UTM event and matched application traffic log.											
<i>disable</i>	Disable traffic and application log.											
session-ttl	TTL in seconds for sessions accepted by this policy .	integer	Minimum value: 300 Maximum value: 2764800	0								
srcaddr6 <name>	IPv6 source address objects. Address name.	string	Maximum length: 79									
dstaddr6 <name>	IPv6 destination address objects. Address name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default
groups <name>	Names of group objects. Group name.	string	Maximum length: 79	
users <name>	Names of user objects. Group name.	string	Maximum length: 79	
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-	disable
Option		Description		
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable
Option		Description		
		<i>enable</i>	Enable SSH policy redirect.	
		<i>disable</i>	Disable SSH policy redirect.	
webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63	
webproxy-profile	Name of web proxy profile.	string	Maximum length: 63	
transparent	Enable to use the IP address of the client to connect to the server.	option	-	disable
Option		Description		
		<i>enable</i>	Enable use of IP address of client to connect to server.	
		<i>disable</i>	Disable use of IP address of client to connect to server.	
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-	disable
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	
utm-status	Enable the use of UTM profiles/sensors/lists.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single
	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	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
dlp-sensor	Name of an existing DLP sensor.	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	
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35	
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
replacemsg-override-group	Authentication replacement message override group.	string	Maximum length: 35	
logtraffic-start	Enable/disable policy log traffic start.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			
comments	Optional comments.	var-string	Maximum length: 1023	
redirect-url	Redirect URL for further explicit web proxy processing.	var-string	Maximum length: 1023	
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35	

config firewall dnstranslation

Configure DNS translation.

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

config firewall dnstranslation

Parameter	Description	Type	Size	Default
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

config firewall multicast-policy

Configure multicast NAT policies.

```
config firewall multicast-policy
  Description: Configure multicast NAT policies.
  edit <id>
    set uuid {uuid}
    set name {string}
    set comments {var-string}
    set status [enable|disable]
    set logtraffic [enable|disable]
    set srcintf {string}
    set dstintf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set snat [enable|disable]
    set snat-ip {ipv4-address}
    set dnat {ipv4-address-any}
    set action [accept|deny]
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set auto-asic-offload [enable|disable]
  next
end
```

config firewall multicast-policy

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	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
status	Enable/disable this policy.	option	-	enable
Option	Description			
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-	disable
Option	Description			
	<i>enable</i>	Enable logging traffic accepted by this policy.		
	<i>disable</i>	Disable logging traffic accepted by this policy.		
srcintf	Source interface name.	string	Maximum length: 35	
dstintf	Destination interface name.	string	Maximum length: 35	
srcaddr <name>	Source address objects. Source address objects.	string	Maximum length: 79	
dstaddr <name>	Destination address objects. Destination address objects.	string	Maximum length: 79	
snat	Enable/disable substitution of the outgoing interface IP address for the original source IP address (called source NAT or SNAT).	option	-	disable
Option	Description			
	<i>enable</i>	Enable source NAT.		
	<i>disable</i>	Disable source NAT.		
snat-ip	IPv4 address to be used as the source address for NATed traffic.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
dnat	IPv4 DNAT address used for multicast destination addresses.	ipv4-address-any	Not Specified	0.0.0.0
action	Accept or deny traffic matching the policy.	option	-	accept
	Option	Description		
	<i>accept</i>	Accept traffic matching the policy.		
	<i>deny</i>	Deny or block traffic matching the policy.		
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	65535
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable hardware acceleration offloading.		
	<i>disable</i>	Disable offloading for hardware acceleration.		

config firewall multicast-policy6

Configure IPv6 multicast NAT policies.

```
config firewall multicast-policy6
  Description: Configure IPv6 multicast NAT policies.
  edit <id>
    set uuid {uuid}
    set status [enable|disable]
    set name {string}
    set logtraffic [enable|disable]
    set srcintf {string}
    set dstintf {string}
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
```

```

set action {accept|deny}
set protocol {integer}
set start-port {integer}
set end-port {integer}
set auto-asic-offload {enable|disable}
set comments {var-string}
next
end

```

config firewall multicast-policy6

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
	Option	Description		
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
name	Policy name.	string	Maximum length: 35	
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging traffic accepted by this policy.		
	<i>disable</i>	Disable logging traffic accepted by this policy.		
srcintf	IPv6 source interface name.	string	Maximum length: 35	
dstintf	IPv6 destination interface name.	string	Maximum length: 35	
srcaddr <name>	IPv6 source address name. Address name.	string	Maximum length: 79	
dstaddr <name>	IPv6 destination address name. Address name.	string	Maximum length: 79	
action	Accept or deny traffic matching the policy.	option	-	accept
	Option	Description		
	<i>accept</i>	Accept.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>deny</i>	Deny.		
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535	65535
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable offloading policy traffic for hardware acceleration.		
	<i>disable</i>	Disable offloading policy traffic for hardware acceleration.		
comments	Comment.	var-string	Maximum length: 1023	

config firewall interface-policy

Configure IPv4 interface policies.

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

```

set av-profile-status [enable|disable]
set av-profile {string}
set webfilter-profile-status [enable|disable]
set webfilter-profile {string}
set emailfilter-profile-status [enable|disable]
set emailfilter-profile {string}
set dlp-sensor-status [enable|disable]
set dlp-sensor {string}
next
end

```

config firewall interface-policy

Parameter	Description	Type	Size	Default
status	Enable/disable this policy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
comments	Comments.	var-string	Maximum length: 1023	
logtraffic	Logging type to be used in this policy (Options: all utm disable, Default: utm).	option	-	utm
	Option	Description		
	<i>all</i>	Log all sessions accepted or denied by this policy.		
	<i>utm</i>	Log traffic that has a security profile applied to it.		
	<i>disable</i>	Disable all logging for this policy.		
interface	Monitored interface name from available interfaces.	string	Maximum length: 35	
srcaddr <name>	Address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79	
dstaddr <name>	Address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79	
service <name>	Service object from available options. Service name.	string	Maximum length: 79	
application-list-status	Enable/disable application control.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable application control		
	<i>disable</i>	Disable application control		
application-list	Application list name.	string	Maximum length: 35	
ips-sensor-status	Enable/disable IPS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPS.		
	<i>disable</i>	Disable IPS.		
ips-sensor	IPS sensor name.	string	Maximum length: 35	
dsri	Enable/disable DSRI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
av-profile-status	Enable/disable antivirus.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable antivirus		
	<i>disable</i>	Disable antivirus		
av-profile	Antivirus profile.	string	Maximum length: 35	
webfilter-profile-status	Enable/disable web filtering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable web filtering.		
	<i>disable</i>	Disable web filtering.		
webfilter-profile	Web filter profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
emailfilter-profile-status	Enable/disable email filter.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Email filter.		
	<i>disable</i>	Disable Email filter.		
emailfilter-profile	Email filter profile.	string	Maximum length: 35	
dlp-sensor-status	Enable/disable DLP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dlp-sensor	DLP sensor name.	string	Maximum length: 35	

config firewall interface-policy6

Configure IPv6 interface policies.

```
config firewall interface-policy6
  Description: Configure IPv6 interface policies.
  edit <policyid>
    set status [enable|disable]
    set comments {var-string}
    set logtraffic [all|utm|...]
    set interface {string}
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set service6 <name1>, <name2>, ...
    set application-list-status [enable|disable]
    set application-list {string}
    set ips-sensor-status [enable|disable]
    set ips-sensor {string}
    set dsri [enable|disable]
    set av-profile-status [enable|disable]
    set av-profile {string}
    set webfilter-profile-status [enable|disable]
    set webfilter-profile {string}
    set emailfilter-profile-status [enable|disable]
    set emailfilter-profile {string}
    set dlp-sensor-status [enable|disable]
    set dlp-sensor {string}
  next
end
```

config firewall interface-policy6

Parameter	Description	Type	Size	Default								
status	Enable/disable this policy.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable this policy.</td></tr> <tr> <td><i>disable</i></td><td>Disable this policy.</td></tr> </tbody> </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.											
comments	Comments.	var-string	Maximum length: 1023									
logtraffic	Logging type to be used in this policy (Options: all utm disable, Default: utm).	option	-	utm								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
interface	Monitored interface name from available interfaces.	string	Maximum length: 35									
srcaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79									
dstaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79									
service6 <name>	Service name. Address name.	string	Maximum length: 79									
application-list-status	Enable/disable application control.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable application control</td></tr> <tr> <td><i>disable</i></td><td>Disable application control</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control					
Option	Description											
<i>enable</i>	Enable application control											
<i>disable</i>	Disable application control											
application-list	Application list name.	string	Maximum length: 35									
ips-sensor-status	Enable/disable IPS.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IPS.		
	<i>disable</i>	Disable IPS.		
ips-sensor	IPS sensor name.	string	Maximum length: 35	
dsri	Enable/disable DSRI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
av-profile-status	Enable/disable antivirus.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable antivirus		
	<i>disable</i>	Disable antivirus		
av-profile	Antivirus profile.	string	Maximum length: 35	
webfilter-profile-status	Enable/disable web filtering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable web filtering.		
	<i>disable</i>	Disable web filtering.		
webfilter-profile	Web filter profile.	string	Maximum length: 35	
emailfilter-profile-status	Enable/disable email filter.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Email filter.		
	<i>disable</i>	Disable Email filter.		
emailfilter-profile	Email filter profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
dlp-sensor-status	Enable/disable DLP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dlp-sensor	DLP sensor name.	string	Maximum length: 35	

config firewall DoS-policy

Configure IPv4 DoS policies.

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

config firewall DoS-policy

Parameter	Description	Type	Size	Default
status	Enable/disable this policy.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
name	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
interface	Incoming interface name from available interfaces.	string	Maximum length: 35	
srcaddr <name>	Source address name from available addresses. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79	
service <name>	Service object from available options. Service name.	string	Maximum length: 79	

config anomaly

Parameter	Description	Type	Size	Default
status	Enable/disable this anomaly.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable this status.		
	<i>enable</i>	Enable this status.		
log	Enable/disable anomaly logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
action	Action taken when the threshold is reached.	option	-	pass
	Option	Description		
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.		
	<i>block</i>	Block traffic if this anomaly is found.		
quarantine	Quarantine method.	option	-	none

Parameter	Description	Type	Size	Default	
	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. . 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.			
threshold	Anomaly threshold. Number of detected instances per minute that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0	
threshold (default)	Number of detected instances per minute which triggers action . Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0	

config firewall DoS-policy6

Configure IPv6 DoS policies.

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

```

        set quarantine-log [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
    next
end
next
end

```

config firewall DoS-policy6

Parameter	Description	Type	Size	Default
status	Enable/disable this policy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
name	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
interface	Incoming interface name from available interfaces.	string	Maximum length: 35	
srcaddr <name>	Source address name from available addresses. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79	
service <name>	Service object from available options. Service name.	string	Maximum length: 79	

config anomaly

Parameter	Description	Type	Size	Default
status	Enable/disable this anomaly.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable this status.		
	<i>enable</i>	Enable this status.		
log	Enable/disable anomaly logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
action	Action taken when the threshold is reached.	option	-	pass
	Option	Description		
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.		
	<i>block</i>	Block traffic if this anomaly is found.		
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. . 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.		
threshold	Anomaly threshold. Number of detected instances per minute that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0
threshold (default)	Number of detected instances per minute which triggers action . Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0

config firewall sniper

Configure sniffer.

```
config firewall sniper
  Description: Configure sniffer.
```

```

edit <id>
  set status [enable|disable]
  set logtraffic [all|utm|...]
  set ipv6 [enable|disable]
  set non-ip [enable|disable]
  set interface {string}
  set host {string}
  set port {string}
  set protocol {string}
  set vlan {string}
  set application-list-status [enable|disable]
  set application-list {string}
  set ips-sensor-status [enable|disable]
  set ips-sensor {string}
  set dsri [enable|disable]
  set av-profile-status [enable|disable]
  set av-profile {string}
  set webfilter-profile-status [enable|disable]
  set webfilter-profile {string}
  set emailfilter-profile-status [enable|disable]
  set emailfilter-profile {string}
  set dlp-sensor-status [enable|disable]
  set dlp-sensor {string}
  set ip-threatfeed-status [enable|disable]
  set ip-threatfeed <name1>, <name2>, ...
  set file-filter-profile-status [enable|disable]
  set file-filter-profile {string}
  set ips-dos-status [enable|disable]
config anomaly
  Description: Configuration method to edit Denial of Service (DoS) anomaly settings.
  edit <name>
    set status [disable|enable]
    set log [enable|disable]
    set action [pass|block]
    set quarantine [none|attacker]
    set quarantine-expiry {user}
    set quarantine-log [disable|enable]
    set threshold {integer}
    set threshold(default) {integer}
  next
end
set max-packet-count {integer}
next
end

```

config firewall sniffer

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of the sniffer.	option	-	enable

Parameter	Description	Type	Size	Default
	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
	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.		
ipv6	Enable/disable sniffing IPv6 packets.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sniffer for IPv6 packets.		
	<i>disable</i>	Disable sniffer for IPv6 packets.		
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sniffer for non-IP packets.		
	<i>disable</i>	Disable sniffer for non-IP packets.		
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35	
host	Hosts to filter for in sniffer traffic .	string	Maximum length: 63	
port	Ports to sniff .	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA .	string	Maximum length: 63	
vlan	List of VLANs to sniff.	string	Maximum length: 63	
application-list-status	Enable/disable application control profile.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
application-list	Name of an existing application list.	string	Maximum length: 35	
ips-sensor-status	Enable/disable IPS sensor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
dsri	Enable/disable DSRI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
av-profile-status	Enable/disable antivirus profile.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
av-profile	Name of an existing antivirus profile.	string	Maximum length: 35	
webfilter-profile-status	Enable/disable web filter profile.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
webfilter-profile	Name of an existing web filter profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
emailfilter-profile-status	Enable/disable emailfilter.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
dlp-sensor-status	Enable/disable DLP sensor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
ip-threatfeed-status	Enable/disable IP threat feed.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ip-threatfeed <name>	Name of an existing IP threat feed. Threat feed name.	string	Maximum length: 79	
file-filter-profile-status	Enable/disable file filter.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
ips-dos-status	Enable/disable IPS DoS anomaly detection.	option	-	disable

Parameter	Description		Type	Size	Default
	Option	Description			
	<i>enable</i>	Enable setting.			
	<i>disable</i>	Disable setting.			
max-packet-count	Maximum packet count .		integer	Minimum value: 1 Maximum value: 10000 **	4000

** Values may differ between models.

config anomaly

Parameter	Description		Type	Size	Default
	Option	Description			
status	Enable/disable this anomaly.		option	-	disable
	<i>disable</i>	Disable this status.			
	<i>enable</i>	Enable this status.			
log	Enable/disable anomaly logging.		option	-	disable
	<i>enable</i>	Enable anomaly logging.			
	<i>disable</i>	Disable anomaly logging.			
action	Action taken when the threshold is reached.		option	-	pass
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.			
	<i>block</i>	Block traffic if this anomaly is found.			
quarantine	Quarantine method.		option	-	none
	<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.			

Parameter	Description	Type	Size	Default
quarantine-expiry	Duration of quarantine. . 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.		
threshold	Anomaly threshold. Number of detected instances per minute that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0
threshold (default)	Number of detected instances per minute which triggers action . Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0

config firewall acl



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64, FortiWiFi 61F.

Configure IPv4 access control list.

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

config firewall acl

Parameter	Description	Type	Size	Default
status	Enable/disable access control list status.	option	-	enable
Option		Description		
		enable Enable access control list status.		
		disable Disable access control list status.		
name	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
interface	Interface name.	string	Maximum length: 35	
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79	
service <name>	Service name. Service name.	string	Maximum length: 79	

config firewall acl6



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64, FortiWiFi 61F.

Configure IPv6 access control list.

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

config firewall acl6

Parameter	Description	Type	Size	Default
status	Enable/disable access control list status.	option	-	enable
Option		Description		
		enable Enable access control list status.		
		disable Disable access control list status.		
name	Policy name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
interface	Interface name.	string	Maximum length: 35	
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79	
service <name>	Service name. Service name.	string	Maximum length: 79	

config firewall central-snat-map

Configure IPv4 and IPv6 central SNAT policies.

```
config firewall central-snat-map
  Description: Configure IPv4 and IPv6 central SNAT policies.
  edit <policyid>
    set uuid {uuid}
    set status [enable|disable]
    set type [ipv4|ipv6]
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set orig-addr <name1>, <name2>, ...
    set orig-addr6 <name1>, <name2>, ...
    set dst-addr <name1>, <name2>, ...
    set dst-addr6 <name1>, <name2>, ...
    set protocol {integer}
    set orig-port {user}
    set nat [disable|enable]
    set nat46 [enable|disable]
    set nat64 [enable|disable]
    set nat-ippool <name1>, <name2>, ...
    set nat-ippool6 <name1>, <name2>, ...
    set nat-port {user}
    set comments {var-string}
```

```
next  
end
```

config firewall central-snat-map

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						
status	Enable/disable the active status of this policy.	option	-	enable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enable this policy.</td></tr><tr><td>disable</td><td>Disable this policy.</td></tr></tbody></table>	Option	Description	enable	Enable this policy.	disable	Disable this policy.			
Option	Description									
enable	Enable this policy.									
disable	Disable this policy.									
type	IPv4/IPv6 source NAT.	option	-	ipv4						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>ipv4</td><td>Perform IPv4 source NAT.</td></tr><tr><td>ipv6</td><td>Perform IPv6 source NAT.</td></tr></tbody></table>	Option	Description	ipv4	Perform IPv4 source NAT.	ipv6	Perform IPv6 source NAT.			
Option	Description									
ipv4	Perform IPv4 source NAT.									
ipv6	Perform IPv6 source NAT.									
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79							
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79							
orig-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79							
orig-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							
protocol	Integer value for the protocol type .	integer	Minimum value: 0 Maximum value: 255	0						
orig-port	Original TCP port (1 to 65535, 0 means any port).	user	Not Specified							

Parameter	Description	Type	Size	Default
nat	Enable/disable source NAT.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable source NAT.		
	<i>enable</i>	Enable source NAT.		
nat46	Enable/disable NAT46.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NAT46.		
	<i>disable</i>	Disable NAT46.		
nat64	Enable/disable NAT64.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable NAT64.		
	<i>disable</i>	Disable NAT64.		
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79	
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IPv6 pool name.	string	Maximum length: 79	
nat-port	Translated port or port range (1 to 65535, 0 means any port).	user	Not Specified	
comments	Comment.	var-string	Maximum length: 1023	

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-cache-capacity {integer}
  set cert-cache-timeout {integer}
  set session-cache-capacity {integer}
  set session-cache-timeout {integer}
  set kxp-queue-threshold {integer}
  set ssl-queue-threshold {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 .	integer	Minimum value: 1 Maximum value: 60	30										
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-	2048										
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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 border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Send empty fragments.</td></tr><tr><td>disable</td><td>Do not send empty fragments.</td></tr></tbody></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 border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>bypass</td><td>Bypass connection.</td></tr><tr><td>drop</td><td>Drop connection.</td></tr></tbody></table>	Option	Description	bypass	Bypass connection.	drop	Drop connection.							
Option	Description													
bypass	Bypass connection.													
drop	Drop connection.													
cert-cache-capacity	Maximum capacity of the host certificate cache .	integer	Minimum value: 0 Maximum value: 500	200										
cert-cache-timeout	Time limit to keep certificate cache .	integer	Minimum value: 1 Maximum value: 120	10										

Parameter	Description	Type	Size	Default
session-cache-capacity	Capacity of the SSL session cache .	integer	Minimum value: 0 Maximum value: 1000	500
session-cache-timeout	Time limit to keep SSL session state .	integer	Minimum value: 1 Maximum value: 60	20
kxp-queue-threshold *	Maximum length of the CP KXP queue. When the queue becomes full, the proxy switches cipher functions to the main CPU .	integer	Minimum value: 0 Maximum value: 512	16
ssl-queue-threshold *	Maximum length of the CP SSL queue. When the queue becomes full, the proxy switches cipher functions to the main CPU .	integer	Minimum value: 0 Maximum value: 512	32
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable
Option	Description			
enable	Enable use of SSL abbreviated handshake.			
disable	Disable use of SSL abbreviated handshake.			

* This parameter may not exist in some models.

config firewall ip-translation

Configure firewall IP-translation.

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

config firewall ip-translation

Parameter	Description	Type	Size	Default															
type	IP translation type (option: SCTP).	option	-	SCTP															
Option	Description	SCTP	SCTP																
Option	Description																		
SCTP	SCTP																		
startip	Description	type	size	default	First IPv4 address .		ipv4-address-any	Not Specified	0.0.0.0	endip	Final IPv4 address .	ipv4-address-any	Not Specified	0.0.0.0	map-startip	Address to be used as the starting point for translation in the range .	ipv4-address-any	Not Specified	0.0.0.0
startip	Description	type	size	default															
First IPv4 address .		ipv4-address-any	Not Specified	0.0.0.0															
endip	Final IPv4 address .	ipv4-address-any	Not Specified	0.0.0.0															
map-startip	Address to be used as the starting point for translation in the range .	ipv4-address-any	Not Specified	0.0.0.0															

config firewall ipv6-eh-filter

Configure IPv6 extension header filter.

```
config firewall ipv6-eh-filter
  Description: Configure IPv6 extension header filter.
  set hop-opt [enable|disable]
  set dest-opt [enable|disable]
  set hdopt-type {integer}
  set routing [enable|disable]
  set routing-type {integer}
  set fragment [enable|disable]
  set auth [enable|disable]
  set no-next [enable|disable]
end
```

config firewall ipv6-eh-filter

Parameter	Description	Type	Size	Default					
hop-opt	Enable/disable blocking packets with the Hop-by-Hop Options header .	option	-	disable					
Option	Description	enable	Enable blocking packets with the Hop-by-Hop Options header.	disable	Disable blocking packets with the Hop-by-Hop Options header.				
Option	Description								
enable	Enable blocking packets with the Hop-by-Hop Options header.								
disable	Disable blocking packets with the Hop-by-Hop Options header.								
dest-opt	Description	type	size	default	Enable/disable blocking packets with Destination Options headers .		option	-	disable
dest-opt	Description	type	size	default					
Enable/disable blocking packets with Destination Options headers .		option	-	disable					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable blocking packets with Destination Options headers.		
	<i>disable</i>	Disable blocking packets with Destination Options headers.		
hdopt-type	Block specific Hop-by-Hop and/or Destination Option types (max. 7 types, each between 0 and 255).	integer	Minimum value: 0 Maximum value: 255	
routing	Enable/disable blocking packets with Routing headers .	option	-	enable
	Option	Description		
	<i>enable</i>	Block packets with Routing headers.		
	<i>disable</i>	Allow packets with Routing headers.		
routing-type	Block specific Routing header types .	integer	Minimum value: 0 Maximum value: 255	0
fragment	Enable/disable blocking packets with the Fragment header .	option	-	disable
	Option	Description		
	<i>enable</i>	Block packets with the Fragment header.		
	<i>disable</i>	Allow packets with the Fragment header.		
auth	Enable/disable blocking packets with the Authentication header .	option	-	disable
	Option	Description		
	<i>enable</i>	Block packets with the Authentication header.		
	<i>disable</i>	Allow packets with the Authentication header.		
no-next	Enable/disable blocking packets with the No Next header	option	-	disable
	Option	Description		
	<i>enable</i>	Block packets with the No Next header.		
	<i>disable</i>	Allow packets with the No Next header.		

config firewall iprope list

list

```
config firewall iprope list
  Description: list
  set <group_number> {string}
end
```

config firewall iprope list

Parameter	Description	Type	Size	Default
<group_number>	Number, hexadecimal.	string	Maximum length: -1	

config firewall iprope appctrl list

List application control policies.

```
config firewall iprope appctrl list
  Description: List application control policies.
end
```

config firewall iprope appctrl status

Application control policy status.

```
config firewall iprope appctrl status
  Description: Application control policy status.
end
```

config firewall proute

List policy routing.

```
config firewall proute
  Description: List policy routing.
  set <policy route id> {string}
end
```

config firewall proute

Parameter	Description	Type	Size	Default
<policy route id>	Number.	string	Maximum length: -1	

config firewall proute6

List IPv6 policy routing.

```
config firewall proute6
    Description: List IPv6 policy routing.
end
```

ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 437](#)

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 ssl [enable|disable]
  set ssl-cert {string}
  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	
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-	deny

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not		
	<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.		
ssl	Enable/disable the explicit FTPS proxy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the explicit FTPS proxy.		
	<i>disable</i>	Disable the explicit FTPS proxy.		
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35	Fortinet_CA_SSL
ssl-dh-bits	Bit-size of Diffie-Hellman .	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.		
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option	Description		
	<i>high</i>	High encryption. Allow only AES and ChaCha		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		

hardware

This section includes syntax for the following commands:

- [config hardware memory on page 439](#)
- [config hardware nic on page 439](#)
- [config hardware status on page 439](#)
- [config hardware cpu on page 439](#)

config hardware status

Hardware status.

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

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: -1	

icap

This section includes syntax for the following commands:

- [config icap profile on page 442](#)
- [config icap server on page 441](#)

config icap server

Configure ICAP servers.

```
config icap server
  Description: Configure ICAP servers.
  edit <name>
    set ip-version [4|6]
    set ip-address {ipv4-address-any}
    set ip6-address {ipv6-address}
    set port {integer}
    set max-connections {integer}
    set secure [enable|disable]
    set ssl-cert {string}
  next
end
```

config icap server

Parameter	Description	Type	Size	Default
ip-version	IP version.	option	-	4
	Option	Description		
	4	IPv4 ICAP address.		
	6	IPv6 ICAP address.		
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344

Parameter	Description	Type	Size	Default
max-connections	Maximum number of concurrent connections to ICAP server. Must not be less than wad-worker-count.	integer	Minimum value: 1 Maximum value: 65535	100
secure	Enable/disable secure connection to ICAP server.	option	-	disable
Option		Description		
		<i>enable</i> Enable secure connection to ICAP server.		
		<i>disable</i> Disable secure connection to ICAP server.		
ssl-cert	CA certificate name.	string	Maximum length: 255	

config icap profile

Configure ICAP profiles.

```
config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    set replacemsg-group {string}
    set request [disable|enable]
    set response [disable|enable]
    set streaming-content-bypass [disable|enable]
    set preview [disable|enable]
    set preview-data-length {integer}
    set request-server {string}
    set response-server {string}
    set request-failure [error|bypass]
    set response-failure [error|bypass]
    set request-path {string}
    set response-path {string}
    set methods {option1}, {option2}, ...
    set response-req-hdr [disable|enable]
    set respmod-default-action [forward|bypass]
    set icap-block-log [disable|enable]
    config icap-headers
      Description: Configure ICAP forwarded request headers.
      edit <id>
        set name {string}
        set content {string}
        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	
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-	disable
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
Option		Description		
		<i>disable</i> Disable HTTP response passing to ICAP server.		
		<i>enable</i> Enable HTTP response passing to ICAP server.		
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-	disable
Option		Description		
		<i>disable</i> Disable bypassing of ICAP server for streaming content.		
		<i>enable</i> Enable bypassing of ICAP server for streaming content.		
preview	Enable/disable preview of data to ICAP server.	option	-	disable

Parameter	Description	Type	Size	Default	
	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: 35		
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 35		
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error	
	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.			
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		
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-	delete get head options post put trace 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
	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>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	-	disable
	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
	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 .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable UTM log when infection found.		
	<i>enable</i>	Enable UTM log when infection found.		

config icap-headers

Parameter	Description	Type	Size	Default
name	HTTP forwarded header name.	string	Maximum length: 79	
content	HTTP header content.	string	Maximum length: 255	
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
host	Address object for the host.	string	Maximum length: 79	
action	Action to be taken for ICAP server.	option	-	forward
Parameter	Description	Type	Size	Default
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	0 **

** Values may differ between models.

config header-group

Parameter	Description	Type	Size	Default
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.			

ips

This section includes syntax for the following commands:

- [config ips settings on page 461](#)
- [config ips global on page 458](#)
- [config ips sensor on page 448](#)
- [config ips rule-settings on page 456](#)
- [config ips session on page 462](#)
- [config ips custom on page 456](#)
- [config ips decoder on page 453](#)
- [config ips view-map on page 452](#)
- [config ips rule on page 454](#)

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 cve <cve-entry1>, <cve-entry2>, ...
                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								
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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								
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. set protocol ? lists available protocols. all includes all protocols. other includes all unlisted protocols.	user	Not Specified	all								
os	Operating systems to be protected. all includes all operating systems. other includes all unlisted operating systems.	user	Not Specified	all								
application	Applications to be protected. set application ? lists available applications. all includes all applications. other includes all unlisted applications.	user	Not Specified	all								
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor CVE IDs or CVE wildcards.	string	Maximum length: 19									
status	Status of the signatures included in filter. default enables the filter and only use filters with default status of enable. Filters with default status of disable will not be used.	option	-	default								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable status of selected rules.</td></tr> <tr> <td><i>enable</i></td><td>Enable status of selected rules.</td></tr> <tr> <td><i>default</i></td><td>Default.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable status of selected rules.	<i>enable</i>	Enable status of selected rules.	<i>default</i>	Default.
Option	Description											
<i>disable</i>	Disable status of selected rules.											
<i>enable</i>	Enable status of selected rules.											
<i>default</i>	Default.											
log	Enable/disable logging of signatures included in filter.	option	-	enable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable logging of selected rules.</td></tr> <tr> <td><i>enable</i></td><td>Enable logging of selected rules.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable logging of selected rules.	<i>enable</i>	Enable logging of selected rules.		
Option	Description											
<i>disable</i>	Disable logging of selected rules.											
<i>enable</i>	Enable logging of selected rules.											

Parameter	Description	Type	Size	Default
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
	Option	Description		
	<i>disable</i>	Disable packet logging of selected rules.		
	<i>enable</i>	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
	Option	Description		
	<i>disable</i>	Disable logging of detailed attack context.		
	<i>enable</i>	Enable logging of detailed attack context.		
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

Parameter	Description	Type	Size	Default
	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.		
	<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. . 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 exempt-ip

Parameter	Description	Type	Size	Default
src-ip	Source IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0
dst-ip	Destination IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0

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 [firewall|interface|...]
    next
end

```

config ips view-map

Parameter	Description	Type	Size	Default
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.			
<i>interface</i>	Interface policy.			
<i>interface6</i>	Interface policy6.			
<i>sniffer</i>	Sniffer policy.			
<i>sniffer6</i>	Sniffer policy6.			
<i>explicit</i>	explicit proxy policy.			

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 parameter

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

config ips rule

Configure IPS rules.

```
config ips rule
  Description: Configure IPS rules.
  edit <name>
    set status [disable|enable]
    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
status	Enable/disable status.	option	-	enable
Option	Description			
<i>disable</i>	Disable status.			
<i>enable</i>	Enable status.			

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
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 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						
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable status.</td></tr> <tr> <td><i>enable</i></td><td>Enable status.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable logging.</td></tr> <tr> <td><i>enable</i></td><td>Enable logging.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable packet logging.</td></tr> <tr> <td><i>enable</i></td><td>Enable packet logging.</td></tr> </tbody> </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 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 np-accel-mode [none|basic]
  set cp-accel-mode [none|basic|...]
  set deep-app-insp-timeout {integer}
  set deep-app-insp-db-limit {integer}
  set exclude-signatures [none|industrial]
  set packet-log-queue-depth {integer}
  set ngfw-max-scan-range {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

Parameter	Description	Type	Size	Default
	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	-	regular **
	Option	Description		
	<i>regular</i>	IPS regular database package.		
	<i>extended</i>	IPS extended database package.		
traffic-submit	Enable/disable submitting attack data found by this FortiGate to FortiGuard.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable traffic submit.		
	<i>disable</i>	Disable traffic submit.		
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous
	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
	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 **

Parameter	Description	Type	Size	Default								
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0								
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
np-accel-mode *	Acceleration mode for IPS processing by NPx processors.	option	-	basic								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>NPx acceleration disabled.</td></tr> <tr> <td><i>basic</i></td><td>NPx acceleration enabled.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	NPx acceleration disabled.	<i>basic</i>	NPx acceleration enabled.					
Option	Description											
<i>none</i>	NPx acceleration disabled.											
<i>basic</i>	NPx acceleration enabled.											
cp-accel-mode *	IPS Pattern matching acceleration/offloading to CPx processors.	option	-	advanced								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>CPx acceleration/offloading disabled.</td></tr> <tr> <td><i>basic</i></td><td>Offload basic pattern matching to CPx processors.</td></tr> <tr> <td><i>advanced</i></td><td>Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	CPx acceleration/offloading disabled.	<i>basic</i>	Offload basic pattern matching to CPx processors.	<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.			
Option	Description											
<i>none</i>	CPx acceleration/offloading disabled.											
<i>basic</i>	Offload basic pattern matching to CPx processors.											
<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.											
deep-app-insp-timeout	Timeout for Deep application inspection .	integer	Minimum value: 0 Maximum value: 2147483647	0								
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database	integer	Minimum value: 0 Maximum value: 2147483647	0								
exclude-signatures	Excluded signatures.	option	-	industrial								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No signatures excluded.		
	<i>industrial</i>	Exclude industrial signatures.		
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128
ngfw-max-scan-range	NGFW policy-mode app detection threshold.	integer	Minimum value: 0 Maximum value: 4294967295	4096

* This parameter may not exist in some models.

** Values may differ between models.

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	
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 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}
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 .	integer	Minimum value: 1 Maximum value: 255	1
packet-log-post-attack	Number of packets to log after the IPS signature is detected .	integer	Minimum value: 0 Maximum value: 255	0
packet-log-memory	Maximum memory can be used by packet log .	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

config ips session

Session status.

```

config ips session
    Description: Session status.
end

```

ipsec

This section includes syntax for the following commands:

- [config ipsec tunnel on page 463](#)

config ipsec tunnel

IPsec tunnel.

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

log

This section includes syntax for the following commands:

- [config log fortiguard override-filter on page 551](#)
- [config log syslogd3 override-setting on page 505](#)
- [config log fortianalyzer3 override-setting on page 594](#)
- [config log syslogd4 override-setting on page 518](#)
- [config log syslogd4 filter on page 521](#)
- [config log syslogd2 setting on page 488](#)
- [config log fortianalyzer2 override-setting on page 580](#)
- [config log fortianalyzer-cloud override-filter on page 610](#)
- [config log fortianalyzer setting on page 562](#)
- [config log syslogd filter on page 483](#)
- [config log null-device filter on page 555](#)
- [config log fortianalyzer2 override-filter on page 587](#)
- [config log eventfilter on page 542](#)
- [config log syslogd3 filter on page 508](#)
- [config log syslogd4 setting on page 514](#)
- [config log syslogd setting on page 475](#)
- [config log disk filter on page 539](#)
- [config log threat-weight on page 465](#)
- [config log syslogd2 override-setting on page 492](#)
- [config log fortiguard override-setting on page 547](#)
- [config log memory filter on page 531](#)
- [config log syslogd4 override-filter on page 524](#)
- [config log fortiguard setting on page 545](#)
- [config log webtrends filter on page 527](#)
- [config log syslogd override-setting on page 479](#)
- [config log webtrends setting on page 527](#)
- [config log memory global-setting on page 530](#)
- [config log syslogd2 filter on page 496](#)
- [config log fortianalyzer override-filter on page 573](#)
- [config log syslogd3 override-filter on page 511](#)
- [config log fortianalyzer3 override-filter on page 601](#)
- [config log custom-field on page 475](#)
- [config log setting on page 557](#)
- [config log syslogd override-filter on page 485](#)
- [config log syslogd2 override-filter on page 498](#)
- [config log memory setting on page 531](#)
- [config log fortianalyzer filter on page 570](#)
- [config log fortiguard filter on page 549](#)
- [config log null-device setting on page 554](#)

- [config log fortianalyzer3 filter on page 598](#)
- [config log fortianalyzer-cloud override-setting on page 607](#)
- [config log fortianalyzer3 setting on page 590](#)
- [config log gui-display on page 561](#)
- [config log fortianalyzer override-setting on page 566](#)
- [config log fortianalyzer-cloud setting on page 604](#)
- [config log fortianalyzer2 filter on page 584](#)
- [config log fortianalyzer2 setting on page 576](#)
- [config log syslogd3 setting on page 501](#)
- [config log fortianalyzer-cloud filter on page 608](#)
- [config log disk setting on page 534](#)

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 fortiai [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
```

config log threat-weight

Parameter	Description	Type	Size	Default
	Option	Description		
status	Enable/disable the threat weight feature.	option	-	enable
	<i>enable</i>	Enable the threat weight feature.		
	<i>disable</i>	Disable the threat weight feature.		
blocked-connection	Threat weight score for blocked connections.	option	-	high
	<i>Option</i>	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.		

Parameter	Description	Type	Size	Default
failed-connection	Threat weight score for failed connections.	option	-	low
	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
	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
	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.		
	<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 .	integer	Minimum value: 1 Maximum value: 100	5

Parameter	Description	Type	Size	Default
medium	Medium level score value .	integer	Minimum value: 1 Maximum value: 100	10
high	High level score value .	integer	Minimum value: 1 Maximum value: 100	30
critical	Critical level score value .	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.		
fortiai	Threat weight score for FortiAI-detected virus.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus detected by FortiAI.		
	<i>low</i>	Use the low level score for virus detected by FortiAI.		
	<i>medium</i>	Use the medium level score for virus detected by FortiAI.		
	<i>high</i>	Use the high level score for virus detected by FortiAI.		
	<i>critical</i>	Use the critical level score for virus detected by FortiAI.		
file-blocked	Threat weight score for blocked file detected.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked file detected.		
	<i>low</i>	Use the low level score for blocked file detected.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for oversized file detected.		
	<i>low</i>	Use the low level score for oversized file detected.		
	<i>medium</i>	Use the medium level score for oversized file detected.		
	<i>high</i>	Use the high level score for oversized file detected.		
	<i>critical</i>	Use the critical level score for oversized file detected.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
virus-file-type-executable	Threat weight score for virus (filetype executable) detected.	option	-	medium
	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
	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.		
	<i>low</i>	Use the low level score for virus (content disarm) detected.		
	<i>medium</i>	Use the medium level score for virus (content disarm) detected.		
	<i>high</i>	Use the high level score for virus (content disarm) detected.		
	<i>critical</i>	Use the critical level score for virus (content disarm) detected.		
malware-list	Threat weight score for virus (malware list) detected.	option	-	medium
	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
	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
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.		
	<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.		
	<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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
	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
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS info severity events.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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
	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
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS high severity events.		
	<i>low</i>	Use the low level score for IPS high severity events.		
	<i>medium</i>	Use the medium level score for IPS high severity events.		
	<i>high</i>	Use the high level score for IPS high severity events.		
	<i>critical</i>	Use the critical level score for IPS high severity events.		
critical-severity	Threat weight score for IPS critical severity events.	option	-	critical

Parameter	Description	Type	Size	Default
	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
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
country	Country code.	string	Maximum length: 2	
level	Threat weight score for Geolocation-based events.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.		
	<i>low</i>	Use the low level score for Geolocation-based events.		
	<i>medium</i>	Use the medium level score for Geolocation-based events.		
	<i>high</i>	Use the high level score for Geolocation-based events.		
	<i>critical</i>	Use the critical level score for Geolocation-based events.		

config application

Parameter	Description	Type	Size	Default
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0
level	Threat weight score for Application events.	option	-	low
Option	Description			
<i>disable</i>	Disable threat weight scoring for Application events.			
<i>low</i>	Use the low level score for Application events.			
<i>medium</i>	Use the medium level score for Application events.			
<i>high</i>	Use the high level score for Application events.			
<i>critical</i>	Use the critical level score for Application events.			

config 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
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 15 characters).	string	Maximum length: 15	

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|sdwan|...]
set interface {string}
end

```

config log syslog 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.		
	<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
	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.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
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
	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 .	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.		
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			
<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	

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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|sdwan|...]
  set interface {string}
```

end

config log syslogd override-setting

Parameter	Description	Type	Size	Default																				
status	Enable/disable remote syslog logging.	option	-	disable																				
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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 border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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 border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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.			
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.																							

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		

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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.			
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.															
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr> <tr> <td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr> <tr> <td><i>specify</i></td><td>Set outgoing interface manually.</td></tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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 anomaly [enable|disable]
  set voip [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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
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>ztna</i>	Zero trust network access log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
Parameter	Description	Type	Size	Default
Option	Description			
<i>include</i>	Include logs that match the filter.			
<i>exclude</i>	Exclude logs that match the filter.			

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 anomaly [enable|disable]
set voip [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 syslog 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
	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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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|sdwan|...]
set interface {string}
end

```

config log syslogd2 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.			
	<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		
	<i>local4</i>	Reserved for local use.		
	<i>local5</i>	Reserved for local use.		
	<i>local6</i>	Reserved for local use.		
	<i>local7</i>	Reserved for local use.		
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	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.		
priority	Set log transmission priority.	option	-	default

Parameter	Description	Type	Size	Default
	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
	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 .	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.		
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>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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|sdwan|...}
    set interface {string}
end

```

config log syslogd2 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		
	<i>local4</i>	Reserved for local use.		
	<i>local5</i>	Reserved for local use.		
	<i>local6</i>	Reserved for local use.		
	<i>local7</i>	Reserved for local use.		
source-ip	Source IP address of syslog.	string	Maximum length: 63	
format	Log format.	option	-	default
	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.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
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
	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 .	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.		
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>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	

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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 anomaly [enable|disable]
  set voip [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 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
Parameter	Description	Type	Size	Default
Option	Description	Type	Size	Default
	<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	Type	Size	Default
	<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
	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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>ztna</i>	Zero trust network access 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 anomaly [enable|disable]
  set voip [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
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>ztna</i>	Zero trust network access 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 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|sdwan|...]
set interface {string}
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
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		

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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.			
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.															
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr> <tr> <td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr> <tr> <td><i>specify</i></td><td>Set outgoing interface manually.</td></tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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|sdwan|...]
    set interface {string}
end
```

config log syslogd3 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
Option	Description			
enable	Log to remote syslog server.			
disable	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.		
	<i>clock</i>	Clock daemon.		

Parameter	Description	Type	Size	Default
Option				
	<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
Option				
	<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.		
priority	Set log transmission priority.	option	-	default
Option				
	<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
Option				
	<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
	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 .	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.		
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>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	

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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 anomaly [enable|disable]
    set voip [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

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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>ztna</i>	Zero trust network access 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 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 anomaly [enable|disable]
  set voip [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 syslog3 override-filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.																					

Parameter	Description	Type	Size	Default
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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|sdwan|...]
  set interface {string}
end
```

config log syslogd4 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.		
	<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).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0

Parameter	Description	Type	Size	Default												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.			
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.															
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr> <tr> <td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr> <tr> <td><i>specify</i></td><td>Set outgoing interface manually.</td></tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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|sdwan|...}
    set interface {string}
end
```

config log syslogd4 override-setting

Parameter	Description	Type	Size	Default								
status	Enable/disable remote syslog logging.	option	-	disable								
<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Log to remote syslog server.</td></tr><tr><td>disable</td><td>Do not log to remote syslog server.</td></tr></tbody></table>					Option	Description	enable	Log to remote syslog server.	disable	Do not log to remote syslog server.		
Option	Description											
enable	Log to remote syslog server.											
disable	Do not log to remote syslog server.											
server	Address of remote syslog server.	string	Maximum length: 127									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></tbody></table>					Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											

Parameter	Description	Type	Size	Default
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.			
<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.			

Parameter	Description	Type	Size	Default												
source-ip	Source IP address of syslog.	string	Maximum length: 63													
format	Log format.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.															
priority	Set log transmission priority.	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.			
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.															

Parameter	Description	Type	Size	Default
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>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	

config custom-field-name

Parameter	Description	Type	Size	Default
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

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 anomaly [enable|disable]
  set voip [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
	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.		

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
Option	Description			
<i>traffic</i>	Traffic log.			
<i>event</i>	Event log.			
<i>virus</i>	Antivirus log.			
<i>webfilter</i>	Web filter log.			
<i>attack</i>	Attack log.			
<i>spam</i>	Antispam log.			
<i>anomaly</i>	Anomaly log.			
<i>voip</i>	VoIP log.			
<i>dlp</i>	DLP log.			
<i>app-ctrl</i>	Application control log.			
<i>waf</i>	Web application firewall log.			
<i>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>ztna</i>	Zero trust network access 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 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 anomaly [enable|disable]
  set voip [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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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
	Option	Description		
	<i>enable</i>	Enable logging to WebTrends.		
	<i>disable</i>	Disable logging to WebTrends.		
server	Address of the remote WebTrends server.	string	Maximum length: 63	

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 anomaly {enable|disable}
  set voip {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
	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.		

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

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
Option	Description			
<i>traffic</i>	Traffic log.			
<i>event</i>	Event log.			
<i>virus</i>	Antivirus log.			
<i>webfilter</i>	Web filter log.			
<i>attack</i>	Attack log.			
<i>spam</i>	Antispam log.			
<i>anomaly</i>	Anomaly log.			
<i>voip</i>	VoIP log.			
<i>dlp</i>	DLP log.			
<i>app-ctrl</i>	Application control log.			
<i>waf</i>	Web application firewall log.			
<i>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>ztna</i>	Zero trust network access 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 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	31869788 **
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100	95

** Values may differ between models.

config log memory setting

Settings for memory buffer.

```
config log memory setting
  Description: Settings for memory buffer.
    set status [enable|disable]
end
```

config log memory setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to the FortiGate's memory.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable logging to memory.		
	<i>disable</i>	Disable logging to memory.		

** Values may differ between models.

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 anomaly [enable|disable]
    set voip [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 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	-	disable **
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable sniffer traffic 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.		

** Values may differ between models.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 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 uploadaddir {string}
  set uploadatype {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|sdwan|...]
set interface {string}
end

```

config log disk setting

Parameter	Description		Type	Size	Default
	Option	Description			
status	Enable/disable local disk logging.		option	-	disable **
	<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
	<i>enable</i>	Enable IPS packet archiving.			
	<i>disable</i>	Disable IPS packet archiving.			
max-log-file-size	Maximum log file size before rolling .		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
	<i>daily</i>	Check the log file once a day.			
	<i>weekly</i>	Check the log file once a week.			
roll-day	Day of week on which to roll log file.		option	-	sunday
	<i>sunday</i>	Sunday			
	<i>monday</i>	Monday			
	<i>tuesday</i>	Tuesday			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wednesday</i>	Wednesday		
	<i>thursday</i>	Thursday		
	<i>friday</i>	Friday		
	<i>saturday</i>	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 .	option	-	overwrite
	Option	Description		
	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.		
	<i>nolog</i>	Stop logging when the log disk is full.		
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
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
	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

Parameter	Description	Type	Size	Default	
	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 .	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	
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		
uploadaddir	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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<i>ztna</i>	Upload ZTNA log.		
uploadsched	Set the schedule for uploading log files to the FTP server .	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 .	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable FTPS communication.		
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100	95
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	

** Values may differ between models.

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 anomaly [enable|disable]
  set voip [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.		
	<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.		

Parameter	Description	Type	Size	Default
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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]
end
```

config log eventfilter

Parameter	Description	Type	Size	Default
event	Enable/disable event logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable event logging.		
	<i>disable</i>	Disable event logging.		
system	Enable/disable system event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable system event logging.		
	<i>disable</i>	Disable system event logging.		
vpn	Enable/disable VPN event logging.	option	-	enable
	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
	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
	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
	Option	Description		
	<i>enable</i>	Enable wireless event logging.		
	<i>disable</i>	Disable wireless event logging.		
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable WAN optimization event logging.		
	<i>disable</i>	Disable WAN optimization event logging.		

Parameter	Description	Type	Size	Default
endpoint	Enable/disable endpoint event logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable endpoint event logging.		
	<i>disable</i>	Disable endpoint event logging.		
ha	Enable/disable ha event logging.	option	-	enable
	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
	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
	Option	Description		
	<i>enable</i>	Enable Forti-Extender logging.		
	<i>disable</i>	Disable Forti-Extender logging.		
connector	Enable/disable SDN connector logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SDN connector logging.		
	<i>disable</i>	Disable SDN connector logging.		
sdwan	Enable/disable SD-WAN logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SD-WAN logging.		
	<i>disable</i>	Disable SD-WAN logging.		
cifs	Enable/disable CIFS logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable CIFS logging.		
	<i>disable</i>	Disable CIFS logging.		

Parameter	Description	Type	Size	Default
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.			

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 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|sdwan|...]
    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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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	
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiCloud log transmission priority to default.		
	<i>low</i>	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
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-	high
	Option	Description		
	<i>high-medium</i>	Encrypt logs using high and medium encryption.		
	<i>high</i>	Encrypt logs using high encryption.		
	<i>low</i>	Encrypt logs using low encryption.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	default

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	<i>SSLv3.</i>		
	<i>TLSv1</i>	<i>TLSv1.</i>		
	<i>TLSv1-1</i>	<i>TLSv1.1.</i>		
	<i>TLSv1-2</i>	<i>TLSv1.2.</i>		
conn-timeout	FortiGate 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
	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	

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}
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.		
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	
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiCloud log transmission priority to default.		
	<i>low</i>	Set FortiCloud log transmission priority to low.		

Parameter	Description	Type	Size	Default
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0

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 anomaly [enable|disable]
  set voip [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
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.			

Parameter	Description	Type	Size	Default
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
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>ztna</i>	Zero trust network access log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
Parameter	Description	Type	Size	Default
Option	Description			
<i>include</i>	Include logs that match the filter.			
<i>exclude</i>	Exclude logs that match the filter.			

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 anomaly [enable|disable]
set voip [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.		

Parameter	Description	Type	Size	Default
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 null-device setting

Settings for null device logging.

```
config log null-device setting
  Description: Settings for null device logging.
    set status [enable|disable]
end
```

config log null-device setting

Parameter	Description	Type	Size	Default
status	Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		
	<i>disable</i>	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		

config log 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 anomaly [enable|disable]
  set voip [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
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
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>ztna</i>	Zero trust network access log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
Parameter	Description	Type	Size	Default
Option	Description			
<i>include</i>	Include logs that match the filter.			
<i>exclude</i>	Exclude logs that match the filter.			

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 log-invalid-packet [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 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 custom-log-fields <field-id1>, <field-id2>, ...
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable implicit firewall policy logging.		
	<i>disable</i>	Disable implicit firewall policy logging.		
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable implicit firewall policy6 logging.		
	<i>disable</i>	Disable implicit firewall policy6 logging.		
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable invalid packet traffic logging.		
	<i>disable</i>	Disable invalid packet 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	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local-out logging.		
	<i>disable</i>	Disable local-out logging.		
daemon-log	Enable/disable daemon logging.	option	-	disable
	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

Parameter	Description	Type	Size	Default
	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
	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.		
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35	

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
	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 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 certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  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	
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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		

Parameter	Description	Type	Size	Default
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.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		
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	
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

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 certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  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

Parameter	Description	Type	Size	Default
	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
	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	
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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the 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.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		
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	

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr> <tr> <td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr> <tr> <td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr> <tr> <td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr> <tr> <td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr> <tr> <td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr> <tr> <td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr> <tr> <td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
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										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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 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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  set interface {string}
end
```

config log fortianalyzer2 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	-	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	
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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high

Parameter	Description	Type	Size	Default
	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 Proto- version	Minimum supported protocol version for SSL/TLS connections .	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.		
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
	Option	Description		
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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	
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

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 certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  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

Parameter	Description	Type	Size	Default
	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
	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	
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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the 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.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		
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	

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr> <tr> <td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr> <tr> <td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr> <tr> <td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr> <tr> <td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr> <tr> <td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr> <tr> <td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr> <tr> <td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
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										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		

Parameter	Description	Type	Size	Default
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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 override-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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
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.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		

Parameter	Description	Type	Size	Default
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  set interface {string}
end
```

config log fortianalyzer3 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	-	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	
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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high

Parameter	Description	Type	Size	Default
	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 Proto- version	Minimum supported protocol version for SSL/TLS connections .	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.		
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
	Option	Description		
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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	
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

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 certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  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

Parameter	Description	Type	Size	Default
	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
	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	
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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the 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.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		
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	

Parameter	Description	Type	Size	Default										
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr> <tr> <td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr> <tr> <td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr> <tr> <td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr> </tbody> </table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr> <tr> <td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr> <tr> <td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr> </tbody> </table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.					
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr> <tr> <td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.							
Option	Description													
<i>enable</i>	Enable reliable logging to FortiAnalyzer.													
<i>disable</i>	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr> <tr> <td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr> </tbody> </table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.							
Option	Description													
<i>default</i>	Set FortiAnalyzer log transmission priority to default.													
<i>low</i>	Set FortiAnalyzer log transmission priority to low.													
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										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
	<i>ztna</i>	Zero trust network access 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 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 preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  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|sdwan|...]
  set interface {string}
end
```

config log fortianalyzer-cloud 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.		

Parameter	Description	Type	Size	Default
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.		
presharded-key	Presharded-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	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the 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.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		

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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr> <tr> <td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr> <tr> <td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr> <tr> <td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr> </tbody> </table>					Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.
Option	Description													
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.													
<i>realtime</i>	Log directly to FortiAnalyzer in real time.													
<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.													
<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr> <tr> <td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr> <tr> <td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr> </tbody> </table>					Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.		
Option	Description													
<i>daily</i>	Upload log files to FortiAnalyzer once a day.													
<i>weekly</i>	Upload log files to FortiAnalyzer once a week.													
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.													
upload-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										

Parameter	Description	Type	Size	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>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		

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 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 anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [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 filter

Parameter	Description	Type	Size	Default																		
severity	Lowest severity level to log.	option	-	information																		
<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></table>					Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.												
Option	Description																					
<i>enable</i>	Enable forward traffic logging.																					
<i>disable</i>	Disable forward traffic logging.																					

Parameter	Description	Type	Size	Default						
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable anomaly logging.</td></tr> <tr> <td><i>disable</i></td><td>Disable anomaly logging.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable VoIP logging.</td></tr> <tr> <td><i>disable</i></td><td>Disable VoIP logging.</td></tr> </tbody> </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	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable DLP archive logging.</td></tr> <tr> <td><i>disable</i></td><td>Disable DLP archive logging.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									

config free-style

Parameter	Description	Type	Size	Default
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>ztna</i>	Zero trust network access log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
Parameter	Description	Type	Size	Default
Option	Description			
<i>include</i>	Include logs that match the filter.			
<i>exclude</i>	Exclude logs that match the filter.			

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 anomaly [enable|disable]
set voip [enable|disable]
set dlp-archive [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
	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
	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.		
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.		

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>ztna</i>	Zero trust network access 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.		

mgmt-data

This section includes syntax for the following commands:

- [config mgmt-data status on page 614](#)

config mgmt-data status

mgmt-data status.

```
config mgmt-data status
    Description: mgmt-data status.
end
```

router

This section includes syntax for the following commands:

- [config router multicast6 on page 738](#)
- [config router ospf6 on page 662](#)
- [config router prefix-list6 on page 619](#)
- [config router bfd6 on page 742](#)
- [config router auth-path on page 740](#)
- [config router prefix-list on page 618](#)
- [config router access-list on page 615](#)
- [config router ospf on page 647](#)
- [config router isis on page 716](#)
- [config router multicast on page 730](#)
- [config router rip on page 628](#)
- [config router community-list on page 621](#)
- [config router key-chain on page 620](#)
- [config router policy6 on page 644](#)
- [config router ripng on page 634](#)
- [config router policy on page 641](#)
- [config router access-list6 on page 616](#)
- [config router setting on page 741](#)
- [config router bfd on page 741](#)
- [config router multicast-flow on page 729](#)
- [config router bgp on page 676](#)
- [config router route-map on page 622](#)
- [config router info6 on page 740](#)
- [config router static6 on page 645](#)
- [config router info on page 740](#)
- [config router static on page 639](#)
- [config router aspath-list on page 617](#)

config router access-list

Configure access lists.

```
config router access-list
  Description: Configure access lists.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set prefix {user}
```

```

        set wildcard {user}
        set exact-match [enable|disable]
    next
end
next
end

```

config router access-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny this IP address and netmask prefix.	option	-	permit
Parameter	Description	Type	Size	Default
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	
wildcard	Wildcard to define Cisco-style wildcard filter criteria.	user	Not Specified	
exact-match	Enable/disable exact match.	option	-	disable
Parameter	Description	Type	Size	Default

config router access-list6

Configure IPv6 access lists.

```

config router access-list6
    Description: Configure IPv6 access lists.
    edit <name>
        set comments {string}
        config rule
            Description: Rule.
            edit <id>
                set action [permit|deny]
                set prefix6 {user}
                set exact-match [enable|disable]

```

```

        set flags {integer}
    next
end
next
end

```

config router access-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny this IP address and netmask prefix.	option	-	permit
Option		Description		
		permit Permit or allow this IP address and netmask prefix.		
		deny Deny this IP address and netmask prefix.		
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	
exact-match	Enable/disable exact prefix match.	option	-	disable
Option		Description		
		enable Enable exact match.		
		disable Disable exact match.		
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0

config router aspath-list

Configure Autonomous System (AS) path lists.

```

config router aspath-list
    Description: Configure Autonomous System (AS) path lists.
    edit <name>
        config rule
            Description: AS path list rule.
            edit <id>
                set action [deny|permit]

```

```

        set regexp {string}
    next
end
next
end

```

config rule

Parameter	Description		Type	Size	Default
action	Permit or deny route-based operations, based on the route's AS_PATH attribute.		option	-	
	Option	Description			
	<i>deny</i>	Deny route-based operations.			
	<i>permit</i>	Permit route-based operations.			
regexp	Regular-expression to match the Border Gateway Protocol (BGP) AS paths.		string	Maximum length: 63	

config router prefix-list

Configure IPv4 prefix lists.

```

config router prefix-list
    Description: Configure IPv4 prefix lists.
    edit <name>
        set comments {string}
        config rule
            Description: IPv4 prefix list rule.
            edit <id>
                set action [permit|deny]
                set prefix {user}
                set ge {integer}
                set le {integer}
            next
        end
    next
end

```

config router prefix-list

Parameter	Description		Type	Size	Default
comments	Comment.		string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny this IP address and netmask prefix.	option	-	permit
	Option	Description		
	permit	Allow or permit packets that match this rule.		
	deny	Deny packets that match this rule.		
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	0.0.0.0 0.0.0.0
ge	Minimum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 32	
le	Maximum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 32	

config router prefix-list6

Configure IPv6 prefix lists.

```
config router prefix-list6
  Description: Configure IPv6 prefix lists.
  edit <name>
    set comments {string}
    config rule
      Description: IPv6 prefix list rule.
      edit <id>
        set action [permit|deny]
        set prefix6 {user}
        set ge {integer}
        set le {integer}
        set flags {integer}
      next
    end
  next
end
```

config router prefix-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny packets that match this rule.	option	-	permit
	Option	Description		
	permit	Allow or permit packets that match this rule.		
	deny	Deny packets that match this rule.		
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	
ge	Minimum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 128	
le	Maximum prefix length to be matched .	integer	Minimum value: 0 Maximum value: 128	
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0

config router key-chain

Configure key-chain.

```
config router key-chain
  Description: Configure key-chain.
  edit <name>
    config key
      Description: Configuration method to edit key settings.
      edit <id>
        set accept-lifetime {user}
        set send-lifetime {user}
        set key-string {password}
        set algorithm [md5|hmac-sha1|...]
    next
  end
next
end
```

config key

Parameter	Description	Type	Size	Default
accept-lifetime	Lifetime of received authentication key (format: hh:mm:ss day month year).	user	Not Specified	
send-lifetime	Lifetime of sent authentication key (format: hh:mm:ss day month year).	user	Not Specified	
key-string	Password for the key (max. = 64 characters).	password	Not Specified	
algorithm	Cryptographic algorithm.	option	-	md5
Option	Description			
<i>md5</i>	MD5.			
<i>hmac-sha1</i>	HMAC-SHA1.			
<i>hmac-sha256</i>	HMAC-SHA256.			
<i>hmac-sha384</i>	HMAC-SHA384.			
<i>hmac-sha512</i>	HMAC-SHA512.			

config router community-list

Configure community lists.

```
config router community-list
  Description: Configure community lists.
  edit <name>
    set type [standard|expanded]
    config rule
      Description: Community list rule.
      edit <id>
        set action [deny|permit]
        set regexp {string}
        set match {string}
      next
    end
  next
end
```

config router community-list

Parameter	Description	Type	Size	Default
type	Community list type (standard or expanded).	option	-	standard

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>standard</i>	Standard community list type.		
	<i>expanded</i>	Expanded community list type.		

config rule

Parameter	Description	Type	Size	Default
action	Permit or deny route-based operations, based on the route's COMMUNITY attribute.	option	-	
	Option	Description		
	<i>deny</i>	Deny route-based operations.		
	<i>permit</i>	Permit or allow route-based operations.		
regexp	Ordered list of COMMUNITY attributes as a regular expression.	string	Maximum length: 255	
match	Community specifications for matching a reserved community.	string	Maximum length: 255	

config router route-map

Configure route maps.

```
config router route-map
  Description: Configure route maps.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set match-as-path {string}
        set match-community {string}
        set match-community-exact [enable|disable]
        set match-origin [none|egp|...]
        set match-interface {string}
        set match-ip-address {string}
        set match-ip6-address {string}
        set match-ip-nexthop {string}
        set match-ip6-nexthop {string}
        set match-metric {integer}
        set match-route-type [external-type1|external-type2|...]
        set match-tag {integer}
        set match-vrf {integer}
        set set-aggregator-as {integer}
        set set-aggregator-ip {ipv4-address-any}
```

```

        set set-aspath-action [prepend|replace]
        set set-aspath <as1>, <as2>, ...
        set set-atomic-aggregate [enable|disable]
        set set-community-delete {string}
        set set-community <community1>, <community2>, ...
        set set-community-additive [enable|disable]
        set set-dampening-reachability-half-life {integer}
        set set-dampening-reuse {integer}
        set set-dampening-suppress {integer}
        set set-dampening-max-suppress {integer}
        set set-dampening-unreachability-half-life {integer}
        set set-extcommunity-rt <community1>, <community2>, ...
        set set-extcommunity-soo <community1>, <community2>, ...
        set set-ip-nexthop {ipv4-address}
        set set-ip6-nexthop {ipv6-address}
        set set-ip6-nexthop-local {ipv6-address}
        set set-local-preference {integer}
        set set-metric {integer}
        set set-metric-type [external-type1|external-type2|...]
        set set-originator-id {ipv4-address-any}
        set set-origin [none|egp|...]
        set set-tag {integer}
        set set-weight {integer}
        set set-route-tag {integer}
    next
end
next
end

```

config router route-map

Parameter	Description	Type	Size	Default
comments	Optional comments.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
action	Action.	option	-	permit
		Option	Description	
		permit	Permit.	
		deny	Deny.	
match-as-path	Match BGP AS path list.	string	Maximum length: 35	
match-community	Match BGP community list.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
match-community-exact	Enable/disable exact matching of communities.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable exact matching of communities.		
	<i>disable</i>	Disable exact matching of communities.		
match-origin	Match BGP origin code.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>egp</i>	Remote EGP.		
	<i>igp</i>	Local IGP.		
	<i>incomplete</i>	Unknown heritage.		
match-interface	Match interface configuration.	string	Maximum length: 15	
match-ip-address	Match IP address permitted by access-list or prefix-list.	string	Maximum length: 35	
match-ip6-address	Match IPv6 address permitted by access-list6 or prefix-list6.	string	Maximum length: 35	
match-ip-nexthop	Match next hop IP address passed by access-list or prefix-list.	string	Maximum length: 35	
match-ip6-nexthop	Match next hop IPv6 address passed by access-list6 or prefix-list6.	string	Maximum length: 35	
match-metric	Match metric for redistribute routes.	integer	Minimum value: 0 Maximum value: 4294967295	
match-route-type	Match route type.	option	-	
	Option	Description		
	<i>external-type1</i>	External type 1.		
	<i>external-type2</i>	External type 2.		
	<i>none</i>	No type specified.		

Parameter	Description	Type	Size	Default						
match-tag	Match tag.	integer	Minimum value: 0 Maximum value: 4294967295							
match-vrf	Match VRF ID.	integer	Minimum value: 0 Maximum value: 31							
set-aggregator-as	BGP aggregator AS.	integer	Minimum value: 0 Maximum value: 4294967295	0						
set-aggregator-ip	BGP aggregator IP.	ipv4-address-any	Not Specified	0.0.0.0						
set-aspath-action	Specify preferred action of set-aspath.	option	-	prepend						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>prepend</i></td><td>Prepend.</td></tr> <tr> <td><i>replace</i></td><td>Replace.</td></tr> </tbody> </table>	Option	Description	<i>prepend</i>	Prepend.	<i>replace</i>	Replace.			
Option	Description									
<i>prepend</i>	Prepend.									
<i>replace</i>	Replace.									
set-aspath <as>	Prepend BGP AS path attribute. AS number (0 - 4294967295). NOTE: Use quotes for repeating numbers, e.g.: "1 1 2"	string	Maximum length: 79							
set-atomic-aggregate	Enable/disable BGP atomic aggregate attribute.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable BGP atomic aggregate attribute.</td></tr> <tr> <td><i>disable</i></td><td>Disable BGP atomic aggregate attribute.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable BGP atomic aggregate attribute.	<i>disable</i>	Disable BGP atomic aggregate attribute.			
Option	Description									
<i>enable</i>	Enable BGP atomic aggregate attribute.									
<i>disable</i>	Disable BGP atomic aggregate attribute.									
set-community-delete	Delete communities matching community list.	string	Maximum length: 35							
set-community <community>	BGP community attribute. Attribute: AA AA:NN internet local-AS no-advertise no-export.	string	Maximum length: 79							
set-community-additive	Enable/disable adding set-community to existing community.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable adding set-community to existing community.		
	disable	Disable adding set-community to existing community.		
set-dampening-reachability-half-life	Reachability half-life time for the penalty .	integer	Minimum value: 0 Maximum value: 45	0
set-dampening-reuse	Value to start reusing a route .	integer	Minimum value: 0 Maximum value: 20000	0
set-dampening-suppress	Value to start suppressing a route .	integer	Minimum value: 0 Maximum value: 20000	0
set-dampening-max-suppress	Maximum duration to suppress a route .	integer	Minimum value: 0 Maximum value: 255	0
set-dampening-unreachability-half-life	Unreachability Half-life time for the penalty	integer	Minimum value: 0 Maximum value: 45	0
set-extcommunity-rt <community>	Route Target extended community. AA:NN.	string	Maximum length: 79	
set-extcommunity-soo <community>	Site-of-Origin extended community. AA:NN	string	Maximum length: 79	
set-ip-nexthop	IP address of next hop.	ipv4-address	Not Specified	
set-ip6-nexthop	IPv6 global address of next hop.	ipv6-address	Not Specified	
set-ip6-nexthop-local	IPv6 local address of next hop.	ipv6-address	Not Specified	

Parameter	Description	Type	Size	Default										
set-local-preference	BGP local preference path attribute.	integer	Minimum value: 0 Maximum value: 4294967295											
set-metric	Metric value.	integer	Minimum value: 0 Maximum value: 4294967295											
set-metric-type	Metric type.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>external-type1</i></td><td>External type 1.</td></tr> <tr> <td><i>external-type2</i></td><td>External type 2.</td></tr> <tr> <td><i>none</i></td><td>No type specified.</td></tr> </tbody> </table>	Option	Description	<i>external-type1</i>	External type 1.	<i>external-type2</i>	External type 2.	<i>none</i>	No type specified.					
Option	Description													
<i>external-type1</i>	External type 1.													
<i>external-type2</i>	External type 2.													
<i>none</i>	No type specified.													
set-originator-id	BGP originator ID attribute.	ipv4-address-any	Not Specified											
set-origin	BGP origin code.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>egp</i></td><td>Remote EGP.</td></tr> <tr> <td><i>igp</i></td><td>Local IGP.</td></tr> <tr> <td><i>incomplete</i></td><td>Unknown heritage.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>egp</i>	Remote EGP.	<i>igp</i>	Local IGP.	<i>incomplete</i>	Unknown heritage.			
Option	Description													
<i>none</i>	None.													
<i>egp</i>	Remote EGP.													
<i>igp</i>	Local IGP.													
<i>incomplete</i>	Unknown heritage.													
set-tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295											
set-weight	BGP weight for routing table.	integer	Minimum value: 0 Maximum value: 4294967295											
set-route-tag	Route tag for routing table.	integer	Minimum value: 0 Maximum value: 4294967295											

config router rip

Configure RIP.

```
config router rip
    Description: Configure RIP.
    set default-information-originate [enable|disable]
    set default-metric {integer}
    set max-out-metric {integer}
    set recv-buffer-size {integer}
    config distance
        Description: distance
        edit <id>
            set prefix {ipv4-classnet-any}
            set distance {integer}
            set access-list {string}
        next
    end
    config distribute-list
        Description: Distribute list.
        edit <id>
            set status [enable|disable]
            set direction [in|out]
            set listname {string}
            set interface {string}
        next
    end
    config neighbor
        Description: neighbor
        edit <id>
            set ip {ipv4-address}
        next
    end
    config network
        Description: network
        edit <id>
            set prefix {ipv4-classnet}
        next
    end
    config offset-list
        Description: Offset list.
        edit <id>
            set status [enable|disable]
            set direction [in|out]
            set access-list {string}
            set offset {integer}
            set interface {string}
        next
    end
    set passive-interface <name1>, <name2>, ...
    config redistribute
        Description: Redistribute configuration.
        edit <name>
            set status [enable|disable]
            set metric {integer}
            set routemap {string}
        next
```

```

end
set update-timer {integer}
set timeout-timer {integer}
set garbage-timer {integer}
set version [1|2]
config interface
  Description: RIP interface configuration.
  edit <name>
    set auth-keychain {string}
    set auth-mode [none{text|...}]
    set auth-string {password}
    set receive-version {option1}, {option2}, ...
    set send-version {option1}, {option2}, ...
    set send-version2-broadcast [disable|enable]
    set split-horizon-status [enable|disable]
    set split-horizon [poisoned|regular]
    set flags {integer}
  next
end
end

```

config router rip

Parameter	Description	Type	Size	Default
default-information-originate	Enable/disable generation of default route.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0
recv-buffer-size	Receiving buffer size.	integer	Minimum value: 8129 Maximum value: 2147483647	65536 **
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
update-timer	Update timer in seconds.	integer	Minimum value: 1 Maximum value: 2147483647	30
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	180
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	120
version	RIP version.	option	-	2
Option	Description			
1	Version 1.			
2	Version 2.			

** Values may differ between models.

config distance

Parameter	Description	Type	Size	Default
prefix	Distance prefix.	ipv4-classnet-any	Not Specified	0.0.0.0
distance	Distance .	integer	Minimum value: 1 Maximum value: 255	0
access-list	Access list for route destination.	string	Maximum length: 35	

config distribute-list

Parameter	Description	Type	Size	Default
status	status	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
direction	Distribute list direction.	option	-	out
	Option	Description		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
listname	Distribute access/prefix list name.	string	Maximum length: 35	
interface	Distribute list interface name.	string	Maximum length: 15	

config neighbor

Parameter	Description	Type	Size	Default
ip	IP address.	ipv4-address	Not Specified	0.0.0.0

config network

Parameter	Description	Type	Size	Default
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0

config offset-list

Parameter	Description	Type	Size	Default
status	status	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
direction	Offset list direction.	option	-	out

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
access-list	Access list name.	string	Maximum length: 35	
offset	offset	integer	Minimum value: 1 Maximum value: 16	0
interface	Interface name.	string	Maximum length: 15	

config redistribute

Parameter	Description	Type	Size	Default
status	status	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
routemap	Route map name.	string	Maximum length: 35	

config interface

Parameter	Description	Type	Size	Default
auth-keychain	Authentication key-chain name.	string	Maximum length: 35	
auth-mode	Authentication mode.	option	-	none
	Option	Description		
	<i>none</i>	None.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Text.		
	<i>md5</i>	MD5.		
auth-string	Authentication string/password.	password	Not Specified	
receive-version	Receive version.	option	-	
	Option	Description		
	1	Version 1.		
	2	Version 2.		
send-version	Send version.	option	-	
	Option	Description		
	1	Version 1.		
	2	Version 2.		
send-version2-broadcast	Enable/disable broadcast version 1 compatible packets.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable broadcasting.		
	<i>enable</i>	Enable broadcasting.		
split-horizon-status	Enable/disable split horizon.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
split-horizon	Enable/disable split horizon.	option	-	poisoned
	Option	Description		
	<i>poisoned</i>	Poisoned.		
	<i>regular</i>	Regular.		

Parameter	Description	Type	Size	Default
flags	flags	integer	Minimum value: 0 Maximum value: 255	8

config router ripng

Configure RIPng.

```
config router ripng
    Description: Configure RIPng.
    set default-information-originate [enable|disable]
    set default-metric {integer}
    set max-out-metric {integer}
    config distance
        Description: distance
        edit <id>
            set distance {integer}
            set prefix6 {ipv6-prefix}
            set access-list6 {string}
        next
    end
    config distribute-list
        Description: Distribute list.
        edit <id>
            set status [enable|disable]
            set direction [in|out]
            set listname {string}
            set interface {string}
        next
    end
    config neighbor
        Description: neighbor
        edit <id>
            set ip6 {ipv6-address}
            set interface {string}
        next
    end
    config network
        Description: Network.
        edit <id>
            set prefix {ipv6-prefix}
        next
    end
    config aggregate-address
        Description: Aggregate address.
        edit <id>
            set prefix6 {ipv6-prefix}
        next
    end
    config offset-list
        Description: Offset list.
        edit <id>
```

```

        set status [enable|disable]
        set direction [in|out]
        set access-list6 {string}
        set offset {integer}
        set interface {string}
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
    next
end
set update-timer {integer}
set timeout-timer {integer}
set garbage-timer {integer}
config interface
    Description: RIPng interface configuration.
    edit <name>
        set split-horizon-status [enable|disable]
        set split-horizon [poisoned|regular]
        set flags {integer}
    next
end
end

```

config router ripng

Parameter	Description	Type	Size	Default
default-information-originate	Enable/disable generation of default route.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0

Parameter	Description	Type	Size	Default
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79	
update-timer	Update timer.	integer	Minimum value: 5 Maximum value: 2147483647	30
timeout-timer	Timeout timer.	integer	Minimum value: 5 Maximum value: 2147483647	180
garbage-timer	Garbage timer.	integer	Minimum value: 5 Maximum value: 2147483647	120

config distance

Parameter	Description	Type	Size	Default
distance	Distance .	integer	Minimum value: 1 Maximum value: 255	0
prefix6	Distance prefix6.	ipv6-prefix	Not Specified	::/0
access-list6	Access list for route destination.	string	Maximum length: 35	

config distribute-list

Parameter	Description	Type	Size	Default
status	status	option	-	disable
Option		Description		
<i>enable</i>		Enable setting.		
<i>disable</i>		Disable setting.		
direction	Distribute list direction.	option	-	out

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
listname	Distribute access/prefix list name.	string	Maximum length: 35	
interface	Distribute list interface name.	string	Maximum length: 15	

config neighbor

Parameter	Description	Type	Size	Default
ip6	IPv6 link-local address.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	

config network

Parameter	Description	Type	Size	Default
prefix	Network IPv6 link-local prefix.	ipv6-prefix	Not Specified	::/0

config aggregate-address

Parameter	Description	Type	Size	Default
prefix6	Aggregate address prefix.	ipv6-prefix	Not Specified	::/0

config offset-list

Parameter	Description	Type	Size	Default
status	status	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
direction	Offset list direction.	option	-	out

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
access-list6	IPv6 access list name.	string	Maximum length: 35	
offset	offset	integer	Minimum value: 1 Maximum value: 16	0
interface	Interface name.	string	Maximum length: 15	

config redistribute

Parameter	Description	Type	Size	Default
status	status	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
routemap	Route map name.	string	Maximum length: 35	

config interface

Parameter	Description	Type	Size	Default
split-horizon-status	Enable/disable split horizon.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
split-horizon	Enable/disable split horizon.	option	-	poisoned

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>poisoned</i>	Poisoned.		
	<i>regular</i>	Regular.		
flags	Flags.	integer	Minimum value: 0 Maximum value: 255	8

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 distance {integer}
    set weight {integer}
    set priority {integer}
    set device {string}
    set comment {var-string}
    set blackhole {enable|disable}
    set dynamic-gateway {enable|disable}
    set sdwan-zone <name1>, <name2>, ...
    set dstaddr {string}
    set internet-service {integer}
    set internet-service-custom {string}
    set link-monitor-exempt {enable|disable}
    set vrf {integer}
    set bfd {enable|disable}
  next
end
```

config router static

Parameter	Description	Type	Size	Default
status	Enable/disable this static route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable static route.		
	<i>disable</i>	Disable static route.		

Parameter	Description	Type	Size	Default
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
distance	Administrative distance .	integer	Minimum value: 1 Maximum value: 255	10
weight	Administrative weight .	integer	Minimum value: 0 Maximum value: 255	0
priority	Administrative priority .	integer	Minimum value: 0 Maximum value: 65535	0
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				
<i>enable</i>				
Enable black hole.				
<i>disable</i>				
dynamic-gateway	Enable use of dynamic gateway retrieved from a DHCP or PPP server.	option	-	disable
Option				
<i>enable</i>				
Enable dynamic gateway.				
<i>disable</i>				
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	

Parameter	Description	Type	Size	Default
internet-service	Application ID in the Internet service database.	integer	Minimum value: 0 Maximum value: 4294967295	0
internet-service-custom	Application name in the Internet service custom database.	string	Maximum length: 64	
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable
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)	
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable
Option		Description		
		<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	
		<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).	

config router policy

Configure IPv4 routing policies.

```
config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set input-device <name1>, <name2>, ...
    set input-device-negate {enable|disable}
    set src <subnet1>, <subnet2>, ...
    set srcaddr <name1>, <name2>, ...
    set src-negate {enable|disable}
    set dst <subnet1>, <subnet2>, ...
    set dstaddr <name1>, <name2>, ...
    set dst-negate {enable|disable}
    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 tos {user}
set tos-mask {user}
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
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	
input-device-negate	Enable/disable negation of input device match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negation of input device match.		
	<i>disable</i>	Disable negation of input device match.		
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
srcaddr <name>	Source address name. Address/group name.	string	Maximum length: 79	
src-negate	Enable/disable negating source address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negation.		
	<i>disable</i>	Disable source address negation.		
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79	
dstaddr <name>	Destination address name. Address/group name.	string	Maximum length: 79	
dst-negate	Enable/disable negating destination address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable destination address negation.		
	<i>disable</i>	Disable destination address negation.		

Parameter	Description	Type	Size	Default
action	Action of the policy route.	option	-	permit
	Option	Description		
	<i>deny</i>	Do not search policy route table.		
	<i>permit</i>	Use this policy route for forwarding.		
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start destination port number .	integer	Minimum value: 0 Maximum value: 65535	0
end-port	End destination port number .	integer	Minimum value: 0 Maximum value: 65535	65535
start-source-port	Start source port number .	integer	Minimum value: 0 Maximum value: 65535	0
end-source-port	End source port number .	integer	Minimum value: 0 Maximum value: 65535	65535
gateway	IP address of the gateway.	ipv4-address	Not Specified	0.0.0.0
output-device	Outgoing interface name.	string	Maximum length: 35	
tos	Type of service bit pattern.	user	Not Specified	
tos-mask	Type of service evaluated bits.	user	Not Specified	
status	Enable/disable this policy route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this policy route.		
	<i>disable</i>	Disable this policy route.		
comments	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
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 policy6

Configure IPv6 routing policies.

```
config router policy6
  Description: Configure IPv6 routing policies.
  edit <seq-num>
    set input-device <name1>, <name2>, ...
    set src {ipv6-network}
    set dst {ipv6-network}
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set gateway {ipv6-address}
    set output-device {string}
    set tos {user}
    set tos-mask {user}
    set status [enable|disable]
    set comments {var-string}
  next
end
```

config router policy6

Parameter	Description	Type	Size	Default
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	
src	Source IPv6 prefix.	ipv6-network	Not Specified	::/0
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start destination port number .	integer	Minimum value: 1 Maximum value: 65535	1
end-port	End destination port number .	integer	Minimum value: 1 Maximum value: 65535	65535
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::
output-device	Outgoing interface name.	string	Maximum length: 35	
tos	Type of service bit pattern.	user	Not Specified	
tos-mask	Type of service evaluated bits.	user	Not Specified	
status	Enable/disable this policy route.	option	-	enable
Option	Description			
<i>enable</i>	Enable this policy route.			
<i>disable</i>	Disable this policy route.			
comments	Optional comments.	var-string	Maximum length: 255	

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 distance {integer}
```

```

set priority {integer}
set comment {var-string}
set blackhole [enable|disable]
set dynamic-gateway [enable|disable]
set sdwan-zone <name1>, <name2>, ...
set link-monitor-exempt [enable|disable]
set vrf {integer}
set bfd [enable|disable]
next
end

```

config router static6

Parameter	Description	Type	Size	Default
status	Enable/disable this static route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable static route.		
	<i>disable</i>	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 .	integer	Minimum value: 0 Maximum value: 4294967295	0
distance	Administrative distance .	integer	Minimum value: 1 Maximum value: 255	10
priority	Administrative priority .	integer	Minimum value: 1 Maximum value: 65535	1024
comment	Optional comments.	var-string	Maximum length: 255	
blackhole	Enable/disable black hole.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable black hole.		
	<i>disable</i>	Disable black hole.		
dynamic-gateway	Enable use of dynamic gateway retrieved from Router Advertisement (RA).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dynamic gateway.		
	<i>disable</i>	Disable dynamic gateway.		
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	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)		
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).		
	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).		

config router ospf

Configure OSPF.

```
config router ospf
  Description: Configure OSPF.
  set abr-type [cisco|ibm|...]
  set auto-cost-ref-bandwidth {integer}
  set distance-external {integer}
  set distance-inter-area {integer}
  set distance-intra-area {integer}
  set database-overflow [enable|disable]
```

```

set database-overflow-max-lsas {integer}
set database-overflow-time-to-recover {integer}
set default-information-originate {enable|always|...}
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-route-map {string}
set default-metric {integer}
set distance {integer}
set rfc1583-compatible [enable|disable]
set router-id {ipv4-address-any}
set spf-timers {user}
set bfd [enable|disable]
set log-neighbour-changes [enable|disable]
set distribute-list-in {string}
set distribute-route-map-in {string}
set restart-mode [none|lls|...]
set restart-period {integer}
config area
    Description: OSPF area configuration.
    edit <id>
        set shortcut [disable|enable|...]
        set authentication [none{text|...}]
        set default-cost {integer}
        set nssa-translator-role [candidate|never|...]
        set stub-type [no-summary|summary]
        set type [regular|nssa|...]
        set nssa-default-information-originate [enable|always|...]
        set nssa-default-information-originate-metric {integer}
        set nssa-default-information-originate-metric-type [1|2]
        set nssa-redistribution [enable|disable]
        set comments {var-string}
    config range
        Description: OSPF area range configuration.
        edit <id>
            set prefix {ipv4-classnet-any}
            set advertise [disable|enable]
            set substitute {ipv4-classnet-any}
            set substitute-status [enable|disable]
        next
    end
    config virtual-link
        Description: OSPF virtual link configuration.
        edit <name>
            set authentication [none{text|...}]
            set authentication-key {password}
            set keychain {string}
            set dead-interval {integer}
            set hello-interval {integer}
            set retransmit-interval {integer}
            set transmit-delay {integer}
            set peer {ipv4-address-any}
        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end

```

```

        next
    end
    config filter-list
        Description: OSPF area filter-list configuration.
        edit <id>
            set list {string}
            set direction [in|out]
        next
    end
    next
end
config ospf-interface
    Description: OSPF interface configuration.
    edit <name>
        set comments {var-string}
        set interface {string}
        set ip {ipv4-address}
        set authentication [none{text|...}]
        set authentication-key {password}
        set keychain {string}
        set prefix-length {integer}
        set retransmit-interval {integer}
        set transmit-delay {integer}
        set cost {integer}
        set priority {integer}
        set dead-interval {integer}
        set hello-interval {integer}
        set hello-multiplier {integer}
        set database-filter-out [enable|disable]
        set mtu {integer}
        set mtu-ignore [enable|disable]
        set network-type [broadcast|non-broadcast|...]
        set bfd [global|enable|...]
        set status [disable|enable]
        set resync-timeout {integer}
    config md5-keys
        Description: MD5 key.
        edit <id>
            set key-string {password}
        next
    end
    next
end
config network
    Description: OSPF network configuration.
    edit <id>
        set prefix {ipv4-classnet}
        set area {ipv4-address-any}
        set comments {var-string}
    next
end
config neighbor
    Description: OSPF neighbor configuration are used when OSPF runs on non-broadcast media
    edit <id>
        set ip {ipv4-address}
        set poll-interval {integer}
        set cost {integer}

```

```

        set priority {integer}
    next
end
set passive-interface <name1>, <name2>, ...
config summary-address
    Description: IP address summary configuration.
    edit <id>
        set prefix {ipv4-classnet}
        set tag {integer}
        set advertise [disable|enable]
    next
end
config distribute-list
    Description: Distribute list configuration.
    edit <id>
        set access-list {string}
        set protocol [connected|static|...]
    next
end
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
        set metric-type [1|2]
        set tag {integer}
    next
end
end

```

config router ospf

Parameter	Description	Type	Size	Default
abr-type	Area border router type.	option	-	standard
	Option	Description		
	<i>cisco</i>	Cisco.		
	<i>ibm</i>	IBM.		
	<i>shortcut</i>	Shortcut.		
	<i>standard</i>	Standard.		
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000

Parameter	Description	Type	Size	Default
distance-external	Administrative external distance.	integer	Minimum value: 1 Maximum value: 255	110
distance-inter-area	Administrative inter-area distance.	integer	Minimum value: 1 Maximum value: 255	110
distance-intra-area	Administrative intra-area distance.	integer	Minimum value: 1 Maximum value: 255	110
database-overflow	Enable/disable database overflow.	option	-	disable
Option				
<i>enable</i>				
Enable setting.				
<i>disable</i>				
Disable setting.				
database-overflow-max-lsas	Database overflow maximum LSAs.	integer	Minimum value: 0 Maximum value: 4294967295	10000
database-overflow-time-to-recover	Database overflow time to recover (sec).	integer	Minimum value: 0 Maximum value: 65535	300
default-information-originate	Enable/disable generation of default route.	option	-	disable
Option				
<i>enable</i>				
Enable setting.				
<i>always</i>				
Always advertise the default router.				
<i>disable</i>				
Disable setting.				

Parameter	Description	Type	Size	Default
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10
default-information-metric-type	Default information metric type.	option	-	2
Option		Description		
1		Type 1.		
2		Type 2.		
default-information-route-map	Default information route map.	string	Maximum length: 35	
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10
distance	Distance of the route.	integer	Minimum value: 1 Maximum value: 255	110
rfc1583-compatible	Enable/disable RFC1583 compatibility.	option	-	disable
Option		Description		
<i>enable</i>		Enable setting.		
<i>disable</i>		Disable setting.		
router-id	Router ID.	ipv4-address-any	Not Specified	0.0.0.0
spf-timers	SPF calculation frequency.	user	Not Specified	
bfd	Bidirectional Forwarding Detection (BFD).	option	-	disable
Option		Description		
<i>enable</i>		Enable setting.		
<i>disable</i>		Disable setting.		

Parameter	Description	Type	Size	Default
log-neighbour-changes	Enable logging of OSPF neighbour's changes	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
distribute-list-in	Filter incoming routes.	string	Maximum length: 35	
distribute-route-map-in	Filter incoming external routes by route-map.	string	Maximum length: 35	
restart-mode	OSPF restart mode (graceful or LLS).	option	-	none
	Option	Description		
	<i>none</i>	Hitless restart disabled.		
	<i>lls</i>	LLS mode.		
	<i>graceful-restart</i>	Graceful Restart Mode.		
restart-period	Graceful restart period.	integer	Minimum value: 1 Maximum value: 3600	120
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79	

config area

Parameter	Description	Type	Size	Default
shortcut	Enable/disable shortcut option.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable shortcut option.		
	<i>enable</i>	Enable shortcut option.		
	<i>default</i>	Default shortcut option.		
authentication	Authentication type.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	None.		
	<i>text</i>	Text.		
	<i>message-digest</i>	Message digest.		
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 4294967295	10
nssa-translator-role	NSSA translator role type.	option	-	candidate
	Option	Description		
	<i>candidate</i>	Candidate.		
	<i>never</i>	Never.		
	<i>always</i>	Always.		
stub-type	Stub summary setting.	option	-	summary
	Option	Description		
	<i>no-summary</i>	No summary.		
	<i>summary</i>	Summary.		
type	Area type setting.	option	-	regular
	Option	Description		
	<i>regular</i>	Regular.		
	<i>nssa</i>	NSSA.		
	<i>stub</i>	Stub.		
nssa-default-information-originate	Redistribute, advertise, or do not originate Type-7 default route into NSSA area.	option	-	disable
	Option	Description		
	<i>enable</i>	Redistribute Type-7 default route from routing table.		
	<i>always</i>	Advertise a self-originated Type-7 default route.		
	<i>disable</i>	Do not advertise Type-7 default route.		

Parameter	Description	Type	Size	Default	
nssa-default-information-originate-metric	OSPF default metric.	integer	Minimum value: 0 Maximum value: 16777214	10	
nssa-default-information-originate-metric-type	OSPF metric type for default routes.	option	-	2	
Option		Description			
		1	Type 1.		
		2	Type 2.		
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable	
Option		Description			
		enable	Enable redistribute into NSSA area.		
		disable	Disable redistribute into NSSA area.		
comments	Comment.	var-string	Maximum length: 255		

config range

Parameter	Description	Type	Size	Default	
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0	
advertise	Enable/disable advertise status.	option	-	enable	
Option		Description			
		disable	Disable advertise status.		
		enable	Enable advertise status.		
substitute	Substitute prefix.	ipv4-classnet-any	Not Specified	0.0.0.0	
substitute-status	Enable/disable substitute status.	option	-	disable	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable substitute status.		
	<i>disable</i>	Disable substitute status.		

config virtual-link

Parameter	Description	Type	Size	Default
authentication	Authentication type.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>text</i>	Text.		
	<i>message-digest</i>	Message digest.		
authentication-key	Authentication key.	password	Not Specified	
keychain	Message-digest key-chain name.	string	Maximum length: 35	
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1
peer	Peer IP.	ipv4-address-any	Not Specified	0.0.0.0

config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

config filter-list

Parameter	Description	Type	Size	Default
list	Access-list or prefix-list name.	string	Maximum length: 35	
direction	Direction.	option	-	out
Option		Description		
		<i>in</i> In.		
		<i>out</i> Out.		

config ospf-interface

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
interface	Configuration interface name.	string	Maximum length: 15	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
authentication	Authentication type.	option	-	none
Option		Description		
		<i>none</i> None.		
		<i>text</i> Text.		
		<i>message-digest</i> Message digest.		

Parameter	Description	Type	Size	Default
authentication-key	Authentication key.	password	Not Specified	
keychain	Message-digest key-chain name.	string	Maximum length: 35	
prefix-length	Prefix length.	integer	Minimum value: 0 Maximum value: 32	0
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1
dead-interval	Dead interval.	integer	Minimum value: 0 Maximum value: 65535	0
hello-interval	Hello interval.	integer	Minimum value: 0 Maximum value: 65535	0
hello-multiplier	Number of hello packets within dead interval.	integer	Minimum value: 3 Maximum value: 10	0

Parameter	Description	Type	Size	Default												
database-filter-out	Enable/disable control of flooding out LSAs.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
mtu	MTU for database description packets.	integer	Minimum value: 576 Maximum value: 65535	0												
mtu-ignore	Enable/disable ignore MTU.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
network-type	Network type.	option	-	broadcast												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>broadcast</i></td><td>Broadcast.</td></tr> <tr> <td><i>non-broadcast</i></td><td>Non-broadcast.</td></tr> <tr> <td><i>point-to-point</i></td><td>Point-to-point.</td></tr> <tr> <td><i>point-to-multipoint</i></td><td>Point-to-multipoint.</td></tr> <tr> <td><i>point-to-multipoint-non-broadcast</i></td><td>Point-to-multipoint and non-broadcast.</td></tr> </tbody> </table>	Option	Description	<i>broadcast</i>	Broadcast.	<i>non-broadcast</i>	Non-broadcast.	<i>point-to-point</i>	Point-to-point.	<i>point-to-multipoint</i>	Point-to-multipoint.	<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.			
Option	Description															
<i>broadcast</i>	Broadcast.															
<i>non-broadcast</i>	Non-broadcast.															
<i>point-to-point</i>	Point-to-point.															
<i>point-to-multipoint</i>	Point-to-multipoint.															
<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.															
bfd	Bidirectional Forwarding Detection (BFD).	option	-	global												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>global</i></td><td>Follow global configuration.</td></tr> <tr> <td><i>enable</i></td><td>Enable BFD on this interface.</td></tr> <tr> <td><i>disable</i></td><td>Disable BFD on this interface.</td></tr> </tbody> </table>	Option	Description	<i>global</i>	Follow global configuration.	<i>enable</i>	Enable BFD on this interface.	<i>disable</i>	Disable BFD on this interface.							
Option	Description															
<i>global</i>	Follow global configuration.															
<i>enable</i>	Enable BFD on this interface.															
<i>disable</i>	Disable BFD on this interface.															
status	Enable/disable status.	option	-	enable												

Parameter	Description		Type	Size	Default
	Option	Description			
	<code>disable</code>	Disable status.			
	<code>enable</code>	Enable status.			
resync-timeout	Graceful restart neighbor resynchronization timeout.		integer	Minimum value: 1 Maximum value: 3600	40

config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

config md5-keys

Parameter	Description	Type	Size	Default
key-string	Password for the key.	password	Not Specified	

config network

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
area	Attach the network to area.	ipv4-address-any	Not Specified	0.0.0.0
comments	Comment.	var-string	Maximum length: 255	

config neighbor

Parameter	Description	Type	Size	Default
ip	Interface IP address of the neighbor.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

config summary-address

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0
advertise	Enable/disable advertise status.	option	-	enable
Option		Description		
		<i>disable</i> Disable advertise status.		
		<i>enable</i> Enable advertise status.		

config distribute-list

Parameter	Description	Type	Size	Default
access-list	Access list name.	string	Maximum length: 35	
protocol	Protocol type.	option	-	connected

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>connected</i>	Connected type.		
	<i>static</i>	Static type.		
	<i>rip</i>	RIP type.		

config redistribute

Parameter	Description	Type	Size	Default
status	status	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0
routemap	Route map name.	string	Maximum length: 35	
metric-type	Metric type.	option	-	2
	Option	Description		
	1	Type 1.		
	2	Type 2.		
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0

config router ospf6

Configure IPv6 OSPF.

```
config router ospf6
  Description: Configure IPv6 OSPF.
  set abr-type [cisco|ibm|...]
  set auto-cost-ref-bandwidth {integer}
  set default-information originate [enable|always|...]
```

```

set log-neighbour-changes {enable|disable}
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-route-map {string}
set default-metric {integer}
set router-id {ipv4-address-any}
set spf-timers {user}
set bfd [enable|disable]
config area
    Description: OSPF6 area configuration.
    edit <id>
        set default-cost {integer}
        set nssa-translator-role [candidate|never|...]
        set stub-type [no-summary|summary]
        set type [regular|nssa|...]
        set nssa-default-information-originate [enable|disable]
        set nssa-default-information-originate-metric {integer}
        set nssa-default-information-originate-metric-type [1|2]
        set nssa-redistribution [enable|disable]
        set authentication [none|ah|...]
        set key-rollover-interval {integer}
        set ipsec-auth-alg [md5|sha1|...]
        set ipsec-enc-alg [null|des|...]
    config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
            set auth-key {password}
            set enc-key {password}
        next
    end
config range
    Description: OSPF6 area range configuration.
    edit <id>
        set prefix6 {ipv6-network}
        set advertise [disable|enable]
    next
end
config virtual-link
    Description: OSPF6 virtual link configuration.
    edit <name>
        set dead-interval {integer}
        set hello-interval {integer}
        set retransmit-interval {integer}
        set transmit-delay {integer}
        set peer {ipv4-address-any}
        set authentication [none|ah|...]
        set key-rollover-interval {integer}
        set ipsec-auth-alg [md5|sha1|...]
        set ipsec-enc-alg [null|des|...]
    config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
            set auth-key {password}
            set enc-key {password}
        next
    end
next

```

```

        end
    next
end
config ospf6-interface
    Description: OSPF6 interface configuration.
    edit <name>
        set area-id {ipv4-address-any}
        set interface {string}
        set retransmit-interval {integer}
        set transmit-delay {integer}
        set cost {integer}
        set priority {integer}
        set dead-interval {integer}
        set hello-interval {integer}
        set status [disable|enable]
        set network-type [broadcast|point-to-point|...]
        set bfd [global|enable|...]
        set mtu {integer}
        set mtu-ignore [enable|disable]
        set authentication [none|ah|...]
        set key-rollover-interval {integer}
        set ipsec-auth-alg [md5|sha1|...]
        set ipsec-enc-alg [null|des|...]
    config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
            set auth-key {password}
            set enc-key {password}
        next
    end
config neighbor
    Description: OSPFv3 neighbors are used when OSPFv3 runs on non-broadcast media
    edit <ip6>
        set poll-interval {integer}
        set cost {integer}
        set priority {integer}
    next
end
next
end
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
        set metric-type [1|2]
    next
end
set passive-interface <name1>, <name2>, ...
config summary-address
    Description: IPv6 address summary configuration.
    edit <id>
        set prefix6 {ipv6-network}
        set advertise [disable|enable]
        set tag {integer}
    next

```

```
end  
end
```

config router ospf6

Parameter	Description	Type	Size	Default								
abr-type	Area border router type.	option	-	standard								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>cisco</td><td>Cisco.</td></tr><tr><td>ibm</td><td>IBM.</td></tr><tr><td>standard</td><td>Standard.</td></tr></tbody></table>	Option	Description	cisco	Cisco.	ibm	IBM.	standard	Standard.			
Option	Description											
cisco	Cisco.											
ibm	IBM.											
standard	Standard.											
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000								
default-information-originate	Enable/disable generation of default route.	option	-	disable								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>always</td><td>Always advertise the default router.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></tbody></table>	Option	Description	enable	Enable setting.	always	Always advertise the default router.	disable	Disable setting.			
Option	Description											
enable	Enable setting.											
always	Always advertise the default router.											
disable	Disable setting.											
log-neighbour-changes	Enable logging of OSPFv3 neighbour's changes	option	-	enable								
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></tbody></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10								
default-information-metric-type	Default information metric type.	option	-	2								

Parameter	Description	Type	Size	Default
	Option	Description		
	1	Type 1.		
	2	Type 2.		
default-information-route-map	Default information route map.	string	Maximum length: 35	
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10
router-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0
spf-timers	SPF calculation frequency.	user	Not Specified	
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable
	Option	Description		
	enable	Enable Bidirectional Forwarding Detection (BFD).		
	disable	Disable Bidirectional Forwarding Detection (BFD).		
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79	

config area

Parameter	Description	Type	Size	Default
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 16777215	10
nssa-translator-role	NSSA translator role type.	option	-	candidate

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>candidate</i>	Candidate.		
	<i>never</i>	Never.		
	<i>always</i>	Always.		
stub-type	Stub summary setting.	option	-	summary
	Option	Description		
	<i>no-summary</i>	No summary.		
	<i>summary</i>	Summary.		
type	Area type setting.	option	-	regular
	Option	Description		
	<i>regular</i>	Regular.		
	<i>nssa</i>	NSSA.		
	<i>stub</i>	Stub.		
nssa-default-information-originate	Enable/disable originate type 7 default into NSSA area.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable originate type 7 default into NSSA area.		
	<i>disable</i>	Disable originate type 7 default into NSSA area.		
nssa-default-information-originate-metric	OSPFv3 default metric.	integer	Minimum value: 0 Maximum value: 16777214	10
nssa-default-information-originate-metric-type	OSPFv3 metric type for default routes.	option	-	2
	Option	Description		
	1	Type 1.		
	2	Type 2.		

Parameter	Description	Type	Size	Default
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable redistribute into NSSA area.		
	<i>disable</i>	Disable redistribute into NSSA area.		
authentication	Authentication mode.	option	-	none
	Option	Description		
	<i>none</i>	Disable authentication.		
	<i>ah</i>	Authentication Header.		
	<i>esp</i>	Encapsulating Security Payload.		
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300
ipsec-auth-alg	Authentication algorithm.	option	-	md5
	Option	Description		
	<i>md5</i>	MD5.		
	<i>sha1</i>	SHA1.		
	<i>sha256</i>	SHA256.		
	<i>sha384</i>	SHA384.		
	<i>sha512</i>	SHA512.		
ipsec-enc-alg	Encryption algorithm.	option	-	null
	Option	Description		
	<i>null</i>	No encryption.		
	<i>des</i>	DES.		
	<i>3des</i>	3DES.		
	<i>aes128</i>	AES128.		
	<i>aes192</i>	AES192.		
	<i>aes256</i>	AES256.		

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

config range

Parameter	Description	Type	Size	Default
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0
advertise	Enable/disable advertise status.	option	-	enable
Option				
		Option	Description	
		disable	disable	
		enable	enable	

config virtual-link

Parameter	Description	Type	Size	Default
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10

Parameter	Description	Type	Size	Default
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1
peer	A.B.C.D, peer router ID.	ipv4-address-any	Not Specified	0.0.0.0
authentication	Authentication mode.	option	-	area
Option		Description		
<i>none</i>		Disable authentication.		
<i>ah</i>		Authentication Header.		
<i>esp</i>		Encapsulating Security Payload.		
<i>area</i>		Use the routing area's authentication configuration.		
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300
ipsec-auth-alg	Authentication algorithm.	option	-	md5
Option		Description		
<i>md5</i>		MD5.		
<i>sha1</i>		SHA1.		
<i>sha256</i>		SHA256.		
<i>sha384</i>		SHA384.		
<i>sha512</i>		SHA512.		
ipsec-enc-alg	Encryption algorithm.	option	-	null
Option		Description		
<i>null</i>		No encryption.		
<i>des</i>		DES.		

Parameter	Description		Type	Size	Default
	Option	Description			
	3des	3DES.			
	aes128	AES128.			
	aes192	AES192.			
	aes256	AES256.			

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

config ospf6-interface

Parameter	Description	Type	Size	Default
area-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0
interface	Configuration interface name.	string	Maximum length: 15	
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5

Parameter	Description	Type	Size	Default										
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1										
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0										
priority	priority	integer	Minimum value: 0 Maximum value: 255	1										
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	0										
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	0										
status	Enable/disable OSPF6 routing on this interface.	option	-	enable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable OSPF6 routing.</td></tr> <tr> <td><i>enable</i></td><td>Enable OSPF6 routing.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable OSPF6 routing.	<i>enable</i>	Enable OSPF6 routing.				
Option	Description													
<i>disable</i>	Disable OSPF6 routing.													
<i>enable</i>	Enable OSPF6 routing.													
network-type	Network type.	option	-	broadcast										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>broadcast</i></td><td>broadcast</td></tr> <tr> <td><i>point-to-point</i></td><td>point-to-point</td></tr> <tr> <td><i>non-broadcast</i></td><td>non-broadcast</td></tr> <tr> <td><i>point-to-multipoint</i></td><td>point-to-multipoint</td></tr> </tbody> </table>					Option	Description	<i>broadcast</i>	broadcast	<i>point-to-point</i>	point-to-point	<i>non-broadcast</i>	non-broadcast	<i>point-to-multipoint</i>	point-to-multipoint
Option	Description													
<i>broadcast</i>	broadcast													
<i>point-to-point</i>	point-to-point													
<i>non-broadcast</i>	non-broadcast													
<i>point-to-multipoint</i>	point-to-multipoint													

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>point-to-multipoint-non-broadcast</i></td><td>point-to-multipoint and non-broadcast.</td></tr> </tbody> </table>	Option	Description	<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.									
Option	Description													
<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.													
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	global										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>global</i></td><td>Use global configuration of Bidirectional Forwarding Detection (BFD).</td></tr> <tr> <td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD) on this interface.</td></tr> <tr> <td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD) on this interface.</td></tr> </tbody> </table>	Option	Description	<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.					
Option	Description													
<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).													
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.													
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.													
mtu	MTU for OSPFv3 packets.	integer	Minimum value: 576 Maximum value: 65535	0										
mtu-ignore	Enable/disable ignoring MTU field in DBD packets.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Ignore MTU field in DBD packets.</td></tr> <tr> <td><i>disable</i></td><td>Do not ignore MTU field in DBD packets.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Ignore MTU field in DBD packets.	<i>disable</i>	Do not ignore MTU field in DBD packets.							
Option	Description													
<i>enable</i>	Ignore MTU field in DBD packets.													
<i>disable</i>	Do not ignore MTU field in DBD packets.													
authentication	Authentication mode.	option	-	area										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>Disable authentication.</td></tr> <tr> <td><i>ah</i></td><td>Authentication Header.</td></tr> <tr> <td><i>esp</i></td><td>Encapsulating Security Payload.</td></tr> <tr> <td><i>area</i></td><td>Use the routing area's authentication configuration.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	Disable authentication.	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.	<i>area</i>	Use the routing area's authentication configuration.			
Option	Description													
<i>none</i>	Disable authentication.													
<i>ah</i>	Authentication Header.													
<i>esp</i>	Encapsulating Security Payload.													
<i>area</i>	Use the routing area's authentication configuration.													
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300										
ipsec-auth-alg	Authentication algorithm.	option	-	md5										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>md5</i>	MD5.		
	<i>sha1</i>	SHA1.		
	<i>sha256</i>	SHA256.		
	<i>sha384</i>	SHA384.		
	<i>sha512</i>	SHA512.		
ipsec-enc-alg	Encryption algorithm.	option	-	null
	Option	Description		
	<i>null</i>	No encryption.		
	<i>des</i>	DES.		
	<i>3des</i>	3DES.		
	<i>aes128</i>	AES128.		
	<i>aes192</i>	AES192.		
	<i>aes256</i>	AES256.		

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

config ipsec-keys

Parameter	Description	Type	Size	Default
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

config neighbor

Parameter	Description	Type	Size	Default
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	priority	integer	Minimum value: 0 Maximum value: 255	1

config redistribute

Parameter	Description	Type	Size	Default
status	status	option	-	disable
Option		Description		
		enable Enable setting.		
		disable Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0
routemap	Route map name.	string	Maximum length: 35	
metric-type	Metric type.	option	-	2
Option		Description		
		1 Type 1.		
		2 Type 2.		

config summary-address

Parameter	Description	Type	Size	Default
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0
advertise	Enable/disable advertise status.	option	-	enable
Option	Description			
	<i>disable</i> disable			
	<i>enable</i> enable			
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0

config router bgp

Configure BGP.

```
config router bgp
  Description: Configure BGP.
  set as {integer}
  set router-id {ipv4-address-any}
  set keepalive-timer {integer}
  set holdtime-timer {integer}
  set always-compare-med [enable|disable]
  set bestpath-as-path-ignore [enable|disable]
  set bestpath-cmp-confed-aspath [enable|disable]
  set bestpath-cmp-routerid [enable|disable]
  set bestpath-med-confed [enable|disable]
  set bestpath-med-missing-as-worst [enable|disable]
  set client-to-client-reflection [enable|disable]
  set dampening [enable|disable]
  set deterministic-med [enable|disable]
  set ebgp-multipath [enable|disable]
  set ibgp-multipath [enable|disable]
  set enforce-first-as [enable|disable]
  set fast-external-failover [enable|disable]
  set log-neighbour-changes [enable|disable]
  set network-import-check [enable|disable]
  set ignore-optional-capability [enable|disable]
  set additional-path [enable|disable]
  set additional-path6 [enable|disable]
  set multipath-recursive-distance [enable|disable]
  set recursive-next-hop [enable|disable]
  set cluster-id {ipv4-address-any}
  set confederation-identifier {integer}
  set confederation-peers <peer1>, <peer2>, ...
  set dampening-route-map {string}
```

```

set dampening-reachability-half-life {integer}
set dampening-reuse {integer}
set dampening-suppress {integer}
set dampening-max-suppress-time {integer}
set dampening-unreachability-half-life {integer}
set default-local-preference {integer}
set scan-time {integer}
set distance-external {integer}
set distance-internal {integer}
set distance-local {integer}
set synchronization [enable|disable]
set graceful-restart [enable|disable]
set graceful-restart-time {integer}
set graceful-stalepath-time {integer}
set graceful-update-delay {integer}
set graceful-end-on-timer [enable|disable]
set additional-path-select {integer}
set additional-path-select6 {integer}
config aggregate-address
    Description: BGP aggregate address table.
    edit <id>
        set prefix {ipv4-classnet-any}
        set as-set [enable|disable]
        set summary-only [enable|disable]
    next
end
config aggregate-address6
    Description: BGP IPv6 aggregate address table.
    edit <id>
        set prefix6 {ipv6-prefix}
        set as-set [enable|disable]
        set summary-only [enable|disable]
    next
end
config neighbor
    Description: BGP neighbor table.
    edit <ip>
        set advertisement-interval {integer}
        set allowas-in-enable [enable|disable]
        set allowas-in-enable6 [enable|disable]
        set allowas-in {integer}
        set allowas-in6 {integer}
        set attribute-unchanged {option1}, {option2}, ...
        set attribute-unchanged6 {option1}, {option2}, ...
        set activate [enable|disable]
        set activate6 [enable|disable]
        set bfd [enable|disable]
        set capability-dynamic [enable|disable]
        set capability-orf [none|receive|...]
        set capability-orf6 [none|receive|...]
        set capability-graceful-restart [enable|disable]
        set capability-graceful-restart6 [enable|disable]
        set capability-route-refresh [enable|disable]
        set capability-default-originate [enable|disable]
        set capability-default-originate6 [enable|disable]
        set dont-capability-negotiate [enable|disable]
        set ebgp-enforce-multipath [enable|disable]

```

```
set link-down-failover [enable|disable]
set stale-route [enable|disable]
set next-hop-self [enable|disable]
set next-hop-self6 [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set remove-private-as [enable|disable]
set remove-private-as6 [enable|disable]
set route-reflector-client [enable|disable]
set route-reflector-client6 [enable|disable]
set route-server-client [enable|disable]
set route-server-client6 [enable|disable]
set shutdown [enable|disable]
set soft-reconfiguration [enable|disable]
set soft-reconfiguration6 [enable|disable]
set as-override [enable|disable]
set as-override6 [enable|disable]
set strict-capability-match [enable|disable]
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set ebgp-multipath-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set interface {string}
set maximum-prefix {integer}
set maximum-prefix6 {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set prefix-list-in {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out6 {string}
set remote-as {integer}
set local-as {integer}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in6 {string}
set route-map-out {string}
set route-map-out-preferable {string}
set route-map-out6 {string}
set route-map-out6-preferable {string}
set send-community [standard|extended|...]
set send-community6 [standard|extended|...]
set keep-alive-timer {integer}
```

```

set holdtime-timer {integer}
set connect-timer {integer}
set unsuppress-map {string}
set unsuppress-map6 {string}
set update-source {string}
set weight {integer}
set restart-time {integer}
set additional-path [send|receive|...]
set additional-path6 [send|receive|...]
set adv-additional-path {integer}
set adv-additional-path6 {integer}
set password {password}
config conditional-advertise
    Description: Conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap {string}
        set condition-type [exist|non-exist]
    next
end
config conditional-advertise6
    Description: IPv6 conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap {string}
        set condition-type [exist|non-exist]
    next
end
next
end
config neighbor-group
    Description: BGP neighbor group table.
    edit <name>
        set advertisement-interval {integer}
        set allowas-in-enable [enable|disable]
        set allowas-in-enable6 [enable|disable]
        set allowas-in {integer}
        set allowas-in6 {integer}
        set attribute-unchanged {option1}, {option2}, ...
        set attribute-unchanged6 {option1}, {option2}, ...
        set activate [enable|disable]
        set activate6 [enable|disable]
        set bfd [enable|disable]
        set capability-dynamic [enable|disable]
        set capability-orf [none|receive|...]
        set capability-orf6 [none|receive|...]
        set capability-graceful-restart [enable|disable]
        set capability-graceful-restart6 [enable|disable]
        set capability-route-refresh [enable|disable]
        set capability-default-originate [enable|disable]
        set capability-default-originate6 [enable|disable]
        set dont-capability-negotiate [enable|disable]
        set ebgp-enforce-multipath [enable|disable]
        set link-down-failover [enable|disable]
        set stale-route [enable|disable]
        set next-hop-self [enable|disable]
        set next-hop-self6 [enable|disable]
        set next-hop-self-rr [enable|disable]
        set next-hop-self-rr6 [enable|disable]

```

```
set override-capability [enable|disable]
set passive [enable|disable]
set remove-private-as [enable|disable]
set remove-private-as6 [enable|disable]
set route-reflector-client [enable|disable]
set route-reflector-client6 [enable|disable]
set route-server-client [enable|disable]
set route-server-client6 [enable|disable]
set shutdown [enable|disable]
set soft-reconfiguration [enable|disable]
set soft-reconfiguration6 [enable|disable]
set as-override [enable|disable]
set as-override6 [enable|disable]
set strict-capability-match [enable|disable]
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set ebgp-multipath-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set interface {string}
set maximum-prefix {integer}
set maximum-prefix6 {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set prefix-list-in {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out6 {string}
set remote-as {integer}
set local-as {integer}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in6 {string}
set route-map-out {string}
set route-map-out-preferable {string}
set route-map-out6 {string}
set route-map-out6-preferable {string}
set send-community [standard|extended|...]
set send-community6 [standard|extended|...]
set keep-alive-timer {integer}
set holdtime-timer {integer}
set connect-timer {integer}
set unsuppress-map {string}
set unsuppress-map6 {string}
set update-source {string}
set weight {integer}
```

```

        set restart-time {integer}
        set additional-path [send|receive|...]
        set additional-path6 [send|receive|...]
        set adv-additional-path {integer}
        set adv-additional-path6 {integer}
    next
end
config neighbor-range
    Description: BGP neighbor range table.
    edit <id>
        set prefix {ipv4-classnet}
        set max-neighbor-num {integer}
        set neighbor-group {string}
    next
end
config neighbor-range6
    Description: BGP IPv6 neighbor range table.
    edit <id>
        set prefix6 {ipv6-network}
        set max-neighbor-num {integer}
        set neighbor-group {string}
    next
end
config network
    Description: BGP network table.
    edit <id>
        set prefix {ipv4-classnet}
        set backdoor [enable|disable]
        set route-map {string}
    next
end
config network6
    Description: BGP IPv6 network table.
    edit <id>
        set prefix6 {ipv6-network}
        set backdoor [enable|disable]
        set route-map {string}
    next
end
config redistribute
    Description: BGP IPv4 redistribute table.
    edit <name>
        set status [enable|disable]
        set route-map {string}
    next
end
config redistribute6
    Description: BGP IPv6 redistribute table.
    edit <name>
        set status [enable|disable]
        set route-map {string}
    next
end
config admin-distance
    Description: Administrative distance modifications.
    edit <id>
        set neighbour-prefix {ipv4-classnet}

```

```

        set route-list {string}
        set distance {integer}
    next
end
config vrf-leak
Description: BGP VRF leaking table.
edit <vrf>
    config target
        Description: Target VRF table.
        edit <vrf>
            set route-map {string}
            set interface {string}
        next
    end
next
end
config vrf-leak6
Description: BGP IPv6 VRF leaking table.
edit <vrf>
    config target
        Description: Target VRF table.
        edit <vrf>
            set route-map {string}
            set interface {string}
        next
    end
next
end

```

config router bgp

Parameter	Description	Type	Size	Default
as	Router AS number, valid from 1 to 4294967295, 0 to disable BGP.	integer	Minimum value: 0 Maximum value: 4294967295	0
router-id	Router ID.	ipv4-address-any	Not Specified	
keepalive-timer	Frequency to send keep alive requests.	integer	Minimum value: 0 Maximum value: 65535	60
holdtime-timer	Number of seconds to mark peer as dead.	integer	Minimum value: 3 Maximum value: 65535	180

Parameter	Description	Type	Size	Default						
always-compare-med	Enable/disable always compare MED.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
bestpath-as-path-ignore	Enable/disable ignore AS path.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
bestpath-cmp-confed-aspath	Enable/disable compare federation AS path length.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
bestpath-cmp-routerid	Enable/disable compare router ID for identical EBGP paths.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
bestpath-med-confed	Enable/disable compare MED among confederation paths.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
bestpath-med-missing-as-worst	Enable/disable treat missing MED as least preferred.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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
client-to-client-reflection	Enable/disable client-to-client route reflection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dampening	Enable/disable route-flap dampening.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
deterministic-med	Enable/disable enforce deterministic comparison of MED.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ebgp-multipath	Enable/disable EBGP multi-path.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ibgp-multipath	Enable/disable IBGP multi-path.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
enforce-first-as	Enable/disable enforce first AS for EBGP routes.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
fast-external-failover	Enable/disable reset peer BGP session if link goes down.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
log-neighbour-changes	Enable logging of BGP neighbour's changes	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
network-import-check	Enable/disable ensure BGP network route exists in IGP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ignore-optional-capability	Don't send unknown optional capability notification message	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path	Enable/disable selection of BGP IPv4 additional paths.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
additional-path6	Enable/disable selection of BGP IPv6 additional paths.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
multipath-recursive-distance	Enable/disable use of recursive distance to select multipath.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
recursive-next-hop	Enable/disable recursive resolution of next-hop using BGP route.	option	-	disabled
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
cluster-id	Route reflector cluster ID.	ipv4-address-any	Not Specified	0.0.0.0
confederation-identifier	Confederation identifier.	integer	Minimum value: 1 Maximum value: 4294967295	0
confederation-peers <peer>	Confederation peers. Peer ID.	string	Maximum length: 79	
dampening-route-map	Criteria for dampening.	string	Maximum length: 35	
dampening-reachability-half-life	Reachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45	15
dampening-reuse	Threshold to reuse routes.	integer	Minimum value: 1 Maximum value: 20000	750
dampening-suppress	Threshold to suppress routes.	integer	Minimum value: 1 Maximum value: 20000	2000
dampening-max-suppress-time	Maximum minutes a route can be suppressed.	integer	Minimum value: 1 Maximum value: 255	60

Parameter	Description	Type	Size	Default						
dampening-unreachability-half-life	Unreachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45	15						
default-local-preference	Default local preference.	integer	Minimum value: 0 Maximum value: 4294967295	100						
scan-time	Background scanner interval (sec), 0 to disable it.	integer	Minimum value: 5 Maximum value: 60	60						
distance-external	Distance for routes external to the AS.	integer	Minimum value: 1 Maximum value: 255	20						
distance-internal	Distance for routes internal to the AS.	integer	Minimum value: 1 Maximum value: 255	200						
distance-local	Distance for routes local to the AS.	integer	Minimum value: 1 Maximum value: 255	200						
synchronization	Enable/disable only advertise routes from iBGP if routes present in an IGP.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
graceful-restart	Enable/disable BGP graceful restart capabilities.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
graceful-restart-time	Time needed for neighbors to restart (sec).	integer	Minimum value: 1 Maximum value: 3600	120
graceful-stalepath-time	Time to hold stale paths of restarting neighbor (sec).	integer	Minimum value: 1 Maximum value: 3600	360
graceful-update-delay	Route advertisement/selection delay after restart (sec).	integer	Minimum value: 1 Maximum value: 3600	120
graceful-end-on-timer	Enable/disable to exit graceful restart on timer only.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			
additional-path-select	Number of additional paths to be selected for each IPv4 NLRI.	integer	Minimum value: 2 Maximum value: 255	2
additional-path-select6	Number of additional paths to be selected for each IPv6 NLRI.	integer	Minimum value: 2 Maximum value: 255	2

config aggregate-address

Parameter	Description	Type	Size	Default
prefix	Aggregate prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
as-set	Enable/disable generate AS set path information.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			

Parameter	Description	Type	Size	Default
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config aggregate-address6

Parameter	Description	Type	Size	Default
prefix6	Aggregate IPv6 prefix.	ipv6-prefix	Not Specified	::/0
as-set	Enable/disable generate AS set path information.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config neighbor

Parameter	Description	Type	Size	Default
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 0 Maximum value: 600	30
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-	
	Option	Description		
	<i>as-path</i>	AS path.		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-	
	Option	Description		
	<i>as-path</i>	AS path.		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bfd	Enable/disable BFD for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>receive</i>	Receive ORF lists.		
	<i>send</i>	Send ORF list.		
	<i>both</i>	Send and receive ORF lists.		
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>receive</i>	Receive ORF lists.		
	<i>send</i>	Send ORF list.		
	<i>both</i>	Send and receive ORF lists.		
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ebgp-enforce-multipath	Enable/disable allow multi-hop EBGP neighbors.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
link-down-failover	Enable/disable failover upon link down.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
stale-route	Enable/disable stale route after neighbor down.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
override-capability	Enable/disable override result of capability negotiation.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.					
Option	Description									
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
shutdown	Enable/disable shutdown this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
strict-capability-match	Enable/disable strict capability matching.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35	
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35	
description	Description.	string	Maximum length: 63	
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35	
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35	
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35	
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
ebgp-multipath-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35	
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35	
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35	
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35	
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15	
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix-threshold	Maximum IPv4 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable
Option	Description			
enable	Enable setting.			
disable	Disable setting.			

Parameter	Description	Type	Size	Default
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295	0
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default										
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0										
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35											
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35											
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35											
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35											
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35											
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35											
send-community	IPv4 Send community attribute to neighbor.	option	-	both										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>standard</i></td><td>Standard.</td></tr> <tr> <td><i>extended</i></td><td>Extended.</td></tr> <tr> <td><i>both</i></td><td>Both.</td></tr> <tr> <td><i>disable</i></td><td>Disable</td></tr> </tbody> </table>					Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable
Option	Description													
<i>standard</i>	Standard.													
<i>extended</i>	Extended.													
<i>both</i>	Both.													
<i>disable</i>	Disable													
send-community6	IPv6 Send community attribute to neighbor.	option	-	both										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>standard</i></td><td>Standard.</td></tr> <tr> <td><i>extended</i></td><td>Extended.</td></tr> <tr> <td><i>both</i></td><td>Both.</td></tr> <tr> <td><i>disable</i></td><td>Disable</td></tr> </tbody> </table>					Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable
Option	Description													
<i>standard</i>	Standard.													
<i>extended</i>	Extended.													
<i>both</i>	Both.													
<i>disable</i>	Disable													
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295										

Parameter	Description	Type	Size	Default										
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295										
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535	4294967295										
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15											
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295										
restart-time	Graceful restart delay time .	integer	Minimum value: 0 Maximum value: 3600	0										
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>send</i></td><td>Enable sending additional paths.</td></tr> <tr> <td><i>receive</i></td><td>Enable receiving additional paths.</td></tr> <tr> <td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr> <tr> <td><i>disable</i></td><td>Disable additional paths.</td></tr> </tbody> </table>					Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.
Option	Description													
<i>send</i>	Enable sending additional paths.													
<i>receive</i>	Enable receiving additional paths.													
<i>both</i>	Enable sending and receiving additional paths.													
<i>disable</i>	Disable additional paths.													
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>send</i></td><td>Enable sending additional paths.</td></tr> <tr> <td><i>receive</i></td><td>Enable receiving additional paths.</td></tr> <tr> <td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr> <tr> <td><i>disable</i></td><td>Disable additional paths.</td></tr> </tbody> </table>					Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.
Option	Description													
<i>send</i>	Enable sending additional paths.													
<i>receive</i>	Enable receiving additional paths.													
<i>both</i>	Enable sending and receiving additional paths.													
<i>disable</i>	Disable additional paths.													

Parameter	Description	Type	Size	Default
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2
password	Password used in MD5 authentication.	password	Not Specified	

config conditional-advertise

Parameter	Description	Type	Size	Default
condition-routemap	Name of condition route map.	string	Maximum length: 35	
condition-type	Type of condition.	option	-	exist
Option		Description		
		<i>exist</i> True if condition route map is matched.		
		<i>non-exist</i> True if condition route map is not matched.		

config conditional-advertise6

Parameter	Description	Type	Size	Default
condition-routemap	Name of condition route map.	string	Maximum length: 35	
condition-type	Type of condition.	option	-	exist
Option		Description		
		<i>exist</i> True if condition route map is matched.		
		<i>non-exist</i> True if condition route map is not matched.		

config neighbor-group

Parameter	Description	Type	Size	Default								
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 0 Maximum value: 600	30								
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0								
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	0								
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>as-path</i></td><td>AS path.</td></tr> <tr> <td><i>med</i></td><td>MED.</td></tr> <tr> <td><i>next-hop</i></td><td>Next hop.</td></tr> </tbody> </table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>as-path</i></td><td>AS path.</td></tr> </tbody> </table>	Option	Description	<i>as-path</i>	AS path.							
Option	Description											
<i>as-path</i>	AS path.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>med</i>	MED.		
	<i>next-hop</i>	Next hop.		
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bfd	Enable/disable BFD for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>receive</i>	Receive ORF lists.		
	<i>send</i>	Send ORF list.		
	<i>both</i>	Send and receive ORF lists.		

Parameter	Description	Type	Size	Default										
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>receive</i></td><td>Receive ORF lists.</td></tr> <tr> <td><i>send</i></td><td>Send ORF list.</td></tr> <tr> <td><i>both</i></td><td>Send and receive ORF lists.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ebgp-enforce-multipath	Enable/disable allow multi-hop EBGP neighbors.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
link-down-failover	Enable/disable failover upon link down.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
stale-route	Enable/disable stale route after neighbor down.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-capability	Enable/disable override result of capability negotiation.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
shutdown	Enable/disable shutdown this neighbor.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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						
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
strict-capability-match	Enable/disable strict capability matching.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35							
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35							
description	Description.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35	
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35	
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35	
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35	
ebgp-multipath-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35	
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35	
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35	
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35	
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15	
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix-threshold	Maximum IPv4 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75

Parameter	Description	Type	Size	Default
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100	75
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable
Option		Description		
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable
Option		Description		
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295	0
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35	
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35	
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35	
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35	
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35	
send-community	IPv4 Send community attribute to neighbor.	option	-	both
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
send-community6	IPv6 Send community attribute to neighbor.	option	-	both

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>standard</i>	Standard.		
	<i>extended</i>	Extended.		
	<i>both</i>	Both.		
	<i>disable</i>	Disable		
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535	4294967295
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35	
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35	
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15	
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295
restart-time	Graceful restart delay time .	integer	Minimum value: 0 Maximum value: 3600	0
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>both</i>	Enable sending and receiving additional paths.		
	<i>disable</i>	Disable additional paths.		
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable
	Option	Description		
	<i>send</i>	Enable sending additional paths.		
	<i>receive</i>	Enable receiving additional paths.		
	<i>both</i>	Enable sending and receiving additional paths.		
	<i>disable</i>	Disable additional paths.		
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2

config neighbor-range

Parameter	Description	Type	Size	Default
prefix	Neighbor range prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	

config neighbor-range6

Parameter	Description	Type	Size	Default
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	

config network

Parameter	Description	Type	Size	Default
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
backdoor	Enable/disable route as backdoor.	option	-	disable
Option				
		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
route-map	Route map to modify generated route.	string	Maximum length: 35	

config network6

Parameter	Description	Type	Size	Default
prefix6	Network IPv6 prefix.	ipv6-network	Not Specified	::/0
backdoor	Enable/disable route as backdoor.	option	-	disable
Option				
		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
route-map	Route map to modify generated route.	string	Maximum length: 35	

config redistribute

Parameter	Description	Type	Size	Default
status	Status	option	-	disable

Parameter	Description		Type	Size	Default
	Option	Description			
	<i>enable</i>	Enable setting.			
	<i>disable</i>	Disable setting.			
route-map	Route map name.		string	Maximum length: 35	

config redistribute6

Parameter	Description		Type	Size	Default
	Option	Description			
status	Status		option	-	disable
	<i>enable</i>	Enable setting.			
	<i>disable</i>	Disable setting.			
route-map	Route map name.		string	Maximum length: 35	

config admin-distance

Parameter	Description		Type	Size	Default
neighbour-prefix	Neighbor address prefix.		ipv4-classnet	Not Specified	0.0.0.0
route-list	Access list of routes to apply new distance to.		string	Maximum length: 35	
distance	Administrative distance to apply .		integer	Minimum value: 1 Maximum value: 255	0

config target

Parameter	Description		Type	Size	Default
route-map	Route map of VRF leaking.		string	Maximum length: 35	
interface	Interface which is used to leak routes to target VRF.		string	Maximum length: 15	

config target

Parameter	Description	Type	Size	Default
route-map	Route map of VRF leaking.	string	Maximum length: 35	
interface	Interface which is used to leak routes to target VRF.	string	Maximum length: 15	

config router isis

Configure IS-IS.

```
config router isis
    Description: Configure IS-IS.
    set is-type [level-1-2|level-1|...]
    set adv-passive-only [enable|disable]
    set adv-passive-only6 [enable|disable]
    set auth-mode-11 [password|md5]
    set auth-mode-12 [password|md5]
    set auth-password-11 {password}
    set auth-password-12 {password}
    set auth-keychain-11 {string}
    set auth-keychain-12 {string}
    set auth-sendonly-11 [enable|disable]
    set auth-sendonly-12 [enable|disable]
    set ignore-lsp-errors [enable|disable]
    set lsp-gen-interval-11 {integer}
    set lsp-gen-interval-12 {integer}
    set lsp-refresh-interval {integer}
    set max-lsp-lifetime {integer}
    set spf-interval-exp-11 {user}
    set spf-interval-exp-12 {user}
    set dynamic-hostname [enable|disable]
    set adjacency-check [enable|disable]
    set adjacency-check6 [enable|disable]
    set overload-bit [enable|disable]
    set overload-bit-suppress {option1}, {option2}, ...
    set overload-bit-on-startup {integer}
    set default-originate [enable|disable]
    set default-originate6 [enable|disable]
    set metric-style [narrow|wide|...]
    set redistribute-11 [enable|disable]
    set redistribute-11-list {string}
    set redistribute-12 [enable|disable]
    set redistribute-12-list {string}
    set redistribute6-11 [enable|disable]
    set redistribute6-11-list {string}
    set redistribute6-12 [enable|disable]
    set redistribute6-12-list {string}
    config isis-net
        Description: IS-IS net configuration.
        edit <id>
            set net {user}
```

```

        next
    end
    config isis-interface
        Description: IS-IS interface configuration.
        edit <name>
            set status [enable|disable]
            set status6 [enable|disable]
            set network-type [broadcast|point-to-point|...]
            set circuit-type [level-1-2|level-1|...]
            set csnp-interval-l1 {integer}
            set csnp-interval-l2 {integer}
            set hello-interval-l1 {integer}
            set hello-interval-l2 {integer}
            set hello-multiplier-l1 {integer}
            set hello-multiplier-l2 {integer}
            set hello-padding [enable|disable]
            set lsp-interval {integer}
            set lsp-retransmit-interval {integer}
            set metric-l1 {integer}
            set metric-l2 {integer}
            set wide-metric-l1 {integer}
            set wide-metric-l2 {integer}
            set auth-password-l1 {password}
            set auth-password-l2 {password}
            set auth-keychain-l1 {string}
            set auth-keychain-l2 {string}
            set auth-send-only-l1 [enable|disable]
            set auth-send-only-l2 [enable|disable]
            set auth-mode-l1 [md5|password]
            set auth-mode-l2 [md5|password]
            set priority-l1 {integer}
            set priority-l2 {integer}
            set mesh-group [enable|disable]
            set mesh-group-id {integer}
        next
    end
    config summary-address
        Description: IS-IS summary addresses.
        edit <id>
            set prefix {ipv4-classnet-any}
            set level [level-1-2|level-1|...]
        next
    end
    config summary-address6
        Description: IS-IS IPv6 summary address.
        edit <id>
            set prefix6 {ipv6-prefix}
            set level [level-1-2|level-1|...]
        next
    end
    config redistribute
        Description: IS-IS redistribute protocols.
        edit <protocol>
            set status [enable|disable]
            set metric {integer}
            set metric-type [external|internal]
            set level [level-1-2|level-1|...]

```

```

        set routemap {string}
    next
end
config redistribute6
    Description: IS-IS IPv6 redistribution for routing protocols.
    edit <protocol>
        set status [enable|disable]
        set metric {integer}
        set metric-type [external|internal]
        set level [level-1-2|level-1|...]
        set routemap {string}
    next
end
end

```

config router isis

Parameter	Description	Type	Size	Default
is-type	IS type.	option	-	level-1-2
Option		Description		
<i>level-1-2</i>		Level 1 and 2.		
<i>level-1</i>		Level 1 only.		
<i>level-2-only</i>		Level 2 only.		
adv-passive-only	Enable/disable IS-IS advertisement of passive interfaces only.	option	-	disable
Option		Description		
<i>enable</i>		Advertise passive interfaces only.		
<i>disable</i>		Advertise all IS-IS enabled interfaces.		
adv-passive-only6	Enable/disable IPv6 IS-IS advertisement of passive interfaces only.	option	-	disable
Option		Description		
<i>enable</i>		Advertise passive interfaces only.		
<i>disable</i>		Advertise all IS-IS enabled interfaces.		
auth-mode-l1	Level 1 authentication mode.	option	-	password
Option		Description		
<i>password</i>		Password.		
<i>md5</i>		MD5.		

Parameter	Description	Type	Size	Default						
auth-mode-l2	Level 2 authentication mode.	option	-	password						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>password</i></td><td>Password.</td></tr> <tr> <td><i>md5</i></td><td>MD5.</td></tr> </tbody> </table>	Option	Description	<i>password</i>	Password.	<i>md5</i>	MD5.			
Option	Description									
<i>password</i>	Password.									
<i>md5</i>	MD5.									
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified							
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified							
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35							
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35							
auth-sendonly-l1	Enable/disable level 1 authentication send-only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable level 1 authentication send-only.</td></tr> <tr> <td><i>disable</i></td><td>Disable level 1 authentication send-only.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable level 1 authentication send-only.	<i>disable</i>	Disable level 1 authentication send-only.			
Option	Description									
<i>enable</i>	Enable level 1 authentication send-only.									
<i>disable</i>	Disable level 1 authentication send-only.									
auth-sendonly-l2	Enable/disable level 2 authentication send-only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable level 2 authentication send-only.</td></tr> <tr> <td><i>disable</i></td><td>Disable level 2 authentication send-only.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable level 2 authentication send-only.	<i>disable</i>	Disable level 2 authentication send-only.			
Option	Description									
<i>enable</i>	Enable level 2 authentication send-only.									
<i>disable</i>	Disable level 2 authentication send-only.									
ignore-lsp-errors	Enable/disable ignoring of LSP errors with bad checksums.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable ignoring of LSP errors with bad checksums.</td></tr> <tr> <td><i>disable</i></td><td>Disable ignoring of LSP errors with bad checksums.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable ignoring of LSP errors with bad checksums.	<i>disable</i>	Disable ignoring of LSP errors with bad checksums.			
Option	Description									
<i>enable</i>	Enable ignoring of LSP errors with bad checksums.									
<i>disable</i>	Disable ignoring of LSP errors with bad checksums.									
lsp-gen-interval-l1	Minimum interval for level 1 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30						

Parameter	Description	Type	Size	Default						
lsp-gen-interval-l2	Minimum interval for level 2 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30						
lsp-refresh-interval	LSP refresh time in seconds.	integer	Minimum value: 1 Maximum value: 65535	900						
max-lsp-lifetime	Maximum LSP lifetime in seconds.	integer	Minimum value: 350 Maximum value: 65535	1200						
spf-interval-exp-l1	Level 1 SPF calculation delay.	user	Not Specified							
spf-interval-exp-l2	Level 2 SPF calculation delay.	user	Not Specified							
dynamic-hostname	Enable/disable dynamic hostname.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable dynamic hostname.</td></tr> <tr> <td><i>disable</i></td><td>Disable dynamic hostname.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable dynamic hostname.	<i>disable</i>	Disable dynamic hostname.
Option	Description									
<i>enable</i>	Enable dynamic hostname.									
<i>disable</i>	Disable dynamic hostname.									
adjacency-check	Enable/disable adjacency check.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable adjacency check.</td></tr> <tr> <td><i>disable</i></td><td>Disable adjacency check.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable adjacency check.	<i>disable</i>	Disable adjacency check.
Option	Description									
<i>enable</i>	Enable adjacency check.									
<i>disable</i>	Disable adjacency check.									
adjacency-check6	Enable/disable IPv6 adjacency check.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable IPv6 adjacency check.</td></tr> <tr> <td><i>disable</i></td><td>Disable IPv6 adjacency check.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable IPv6 adjacency check.	<i>disable</i>	Disable IPv6 adjacency check.
Option	Description									
<i>enable</i>	Enable IPv6 adjacency check.									
<i>disable</i>	Disable IPv6 adjacency check.									
overload-bit	Enable/disable signal other routers not to use us in SPF.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable overload bit.		
	<i>disable</i>	Disable overload bit.		
overload-bit-suppress	Suppress overload-bit for the specific prefixes.	option	-	
	Option	Description		
	<i>external</i>	External.		
	<i>interlevel</i>	Inter-level.		
overload-bit-on-startup	Overload-bit only temporarily after reboot.	integer	Minimum value: 5 Maximum value: 86400	0
default-originate	Enable/disable distribution of default route information.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable distribution of default route information.		
	<i>disable</i>	Disable distribution of default route information.		
default-originate6	Enable/disable distribution of default IPv6 route information.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable distribution of default IPv6 route information.		
	<i>disable</i>	Disable distribution of default IPv6 route information.		
metric-style	Use old-style (ISO 10589) or new-style packet formats	option	-	narrow
	Option	Description		
	<i>narrow</i>	Use old style of TLVs with narrow metric.		
	<i>wide</i>	Use new style of TLVs to carry wider metric.		
	<i>transition</i>	Send and accept both styles of TLVs during transition.		
	<i>narrow-transition</i>	Narrow and accept both styles of TLVs during transition.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>narrow-transition-l1</i>	Narrow-transition level-1 only.		
	<i>narrow-transition-l2</i>	Narrow-transition level-2 only.		
	<i>wide-l1</i>	Wide level-1 only.		
	<i>wide-l2</i>	Wide level-2 only.		
	<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.		
	<i>wide-transition-l1</i>	Wide-transition level-1 only.		
	<i>wide-transition-l2</i>	Wide-transition level-2 only.		
	<i>transition-l1</i>	Transition level-1 only.		
	<i>transition-l2</i>	Transition level-2 only.		
redistribute-l1	Enable/disable redistribution of level 1 routes into level 2.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable redistribution of level 1 routes into level 2.		
	<i>disable</i>	Disable redistribution of level 1 routes into level 2.		
redistribute-l1-list	Access-list for route redistribution from l1 to l2.	string	Maximum length: 35	
redistribute-l2	Enable/disable redistribution of level 2 routes into level 1.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable redistribution of level 2 routes into level 1.		
	<i>disable</i>	Disable redistribution of level 2 routes into level 1.		
redistribute-l2-list	Access-list for route redistribution from l2 to l1.	string	Maximum length: 35	
redistribute6-l1	Enable/disable redistribution of level 1 IPv6 routes into level 2.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable redistribution of level 1 IPv6 routes into level 2.		
	<i>disable</i>	Disable redistribution of level 1 IPv6 routes into level 2.		
redistribute6-I1-list	Access-list for IPv6 route redistribution from I1 to I2.	string	Maximum length: 35	
redistribute6-I2	Enable/disable redistribution of level 2 IPv6 routes into level 1.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable redistribution of level 2 IPv6 routes into level 1.		
	<i>disable</i>	Disable redistribution of level 2 IPv6 routes into level 1.		
redistribute6-I2-list	Access-list for IPv6 route redistribution from I2 to I1.	string	Maximum length: 35	

config isis-net

Parameter	Description	Type	Size	Default
net	IS-IS net xx.xxxx.xxxx.xx.	user	Not Specified	

config isis-interface

Parameter	Description	Type	Size	Default
status	Enable/disable interface for IS-IS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable interface for IS-IS.		
	<i>disable</i>	Disable interface for IS-IS.		
status6	Enable/disable IPv6 interface for IS-IS.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv6 interface for IS-IS.		
	<i>disable</i>	Disable IPv6 interface for IS-IS.		
network-type	IS-IS interface's network type	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>broadcast</i>	Broadcast.		
	<i>point-to-point</i>	Point-to-point.		
	<i>loopback</i>	Loopback.		
circuit-type	IS-IS interface's circuit type	option	-	level-1-2
	Option	Description		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
csnp-interval-l1	Level 1 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535	10
csnp-interval-l2	Level 2 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535	10
hello-interval-l1	Level 1 hello interval.	integer	Minimum value: 0 Maximum value: 65535	10
hello-interval-l2	Level 2 hello interval.	integer	Minimum value: 0 Maximum value: 65535	10
hello-multiplier-l1	Level 1 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100	3
hello-multiplier-l2	Level 2 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100	3
hello-padding	Enable/disable padding to IS-IS hello packets.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable padding to IS-IS hello packets.		
	disable	Disable padding to IS-IS hello packets.		
Isp-interval	LSP transmission interval (milliseconds).	integer	Minimum value: 1 Maximum value: 4294967295	33
Isp-retransmit-interval	LSP retransmission interval (sec).	integer	Minimum value: 1 Maximum value: 65535	5
metric-l1	Level 1 metric for interface.	integer	Minimum value: 1 Maximum value: 63	10
metric-l2	Level 2 metric for interface.	integer	Minimum value: 1 Maximum value: 63	10
wide-metric-l1	Level 1 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10
wide-metric-l2	Level 2 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified	
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified	
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
auth-send-only-l1	Enable/disable authentication send-only for level 1 PDUs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable authentication send-only for level 1 PDUs.		
	<i>disable</i>	Disable authentication send-only for level 1 PDUs.		
auth-send-only-l2	Enable/disable authentication send-only for level 2 PDUs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable authentication send-only for level 2 PDUs.		
	<i>disable</i>	Disable authentication send-only for level 2 PDUs.		
auth-mode-l1	Level 1 authentication mode.	option	-	password
	Option	Description		
	<i>md5</i>	MD5.		
	<i>password</i>	Password.		
auth-mode-l2	Level 2 authentication mode.	option	-	password
	Option	Description		
	<i>md5</i>	MD5.		
	<i>password</i>	Password.		
priority-l1	Level 1 priority.	integer	Minimum value: 0 Maximum value: 127	64
priority-l2	Level 2 priority.	integer	Minimum value: 0 Maximum value: 127	64
mesh-group	Enable/disable IS-IS mesh group.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IS-IS mesh group.		
	<i>disable</i>	Disable IS-IS mesh group.		

Parameter	Description	Type	Size	Default
mesh-group-id	Mesh group ID <0-4294967295>, 0: mesh-group blocked.	integer	Minimum value: 0 Maximum value: 4294967295	0

config summary-address

Parameter	Description	Type	Size	Default
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0
level	Level.	option	-	level-2
Option		Description		
<i>level-1-2</i>		Level 1 and 2.		
<i>level-1</i>		Level 1.		
<i>level-2</i>		Level 2.		

config summary-address6

Parameter	Description	Type	Size	Default
prefix6	IPv6 prefix.	ipv6-prefix	Not Specified	::/0
level	Level.	option	-	level-2
Option		Description		
<i>level-1-2</i>		Level 1 and 2.		
<i>level-1</i>		Level 1.		
<i>level-2</i>		Level 2.		

config redistribute

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable.		
	<i>disable</i>	Disable.		
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0
metric-type	Metric type.	option	-	internal
	Option	Description		
	<i>external</i>	External.		
	<i>internal</i>	Internal.		
level	Level.	option	-	level-2
	Option	Description		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
routemap	Route map name.	string	Maximum length: 35	

config redistribute6

Parameter	Description	Type	Size	Default
status	Enable/disable redistribution.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable redistribution.		
	<i>disable</i>	Disable redistribution.		
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0
metric-type	Metric type.	option	-	internal

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>external</i>	External metric type.		
	<i>internal</i>	Internal metric type.		
level	Level.	option	-	level-2
	Option	Description		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
routemap	Route map name.	string	Maximum length: 35	

config router multicast-flow

Configure multicast-flow.

```
config router multicast-flow
  Description: Configure multicast-flow.
  edit <name>
    set comments {string}
    config flows
      Description: Multicast-flow entries.
      edit <id>
        set group-addr {ipv4-address-any}
        set source-addr {ipv4-address-any}
      next
    end
  next
end
```

config router multicast-flow

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	

config flows

Parameter	Description	Type	Size	Default
group-addr	Multicast group IP address.	ipv4-address-any	Not Specified	0.0.0.0
source-addr	Multicast source IP address.	ipv4-address-any	Not Specified	0.0.0.0

config router multicast

Configure router multicast.

```
config router multicast
    Description: Configure router multicast.
    set route-threshold {integer}
    set route-limit {integer}
    set multicast-routing [enable|disable]
    config pim-sm-global
        Description: PIM sparse-mode global settings.
        set message-interval {integer}
        set join-prune-holdtime {integer}
        set accept-register-list {string}
        set accept-source-list {string}
        set bsr-candidate [enable|disable]
        set bsr-interface {string}
        set bsr-priority {integer}
        set bsr-hash {integer}
        set bsr-allow-quick-refresh [enable|disable]
        set cisco-register-checksum [enable|disable]
        set cisco-register-checksum-group {string}
        set cisco-crp-prefix [enable|disable]
        set cisco-ignore-rp-set-priority [enable|disable]
        set register-rp-reachability [enable|disable]
        set register-source [disable|interface|...]
        set register-source-interface {string}
        set register-source-ip {ipv4-address}
        set register-supression {integer}
        set null-register-retries {integer}
        set rp-register-keepalive {integer}
        set spt-threshold [enable|disable]
        set spt-threshold-group {string}
        set ssm [enable|disable]
        set ssm-range {string}
        set register-rate-limit {integer}
    config rp-address
        Description: Statically configure RP addresses.
        edit <id>
            set ip-address {ipv4-address}
            set group {string}
        next
    end
```

```

end
config interface
    Description: PIM interfaces.
    edit <name>
        set ttl-threshold {integer}
        set pim-mode [sparse-mode|dense-mode]
        set passive {enable|disable}
        set bfd {enable|disable}
        set neighbour-filter {string}
        set hello-interval {integer}
        set hello-holdtime {integer}
        set cisco-exclude-genid {enable|disable}
        set dr-priority {integer}
        set propagation-delay {integer}
        set state-refresh-interval {integer}
        set rp-candidate {enable|disable}
        set rp-candidate-group {string}
        set rp-candidate-priority {integer}
        set rp-candidate-interval {integer}
        set multicast-flow {string}
        set static-group {string}
        set rpf-nbr-fail-back {enable|disable}
        set rpf-nbr-fail-back-filter {string}
        config join-group
            Description: Join multicast groups.
            edit <address>
            next
        end
    config igmp
        Description: IGMP configuration options.
        set access-group {string}
        set version [3|2|...]
        set immediate-leave-group {string}
        set last-member-query-interval {integer}
        set last-member-query-count {integer}
        set query-max-response-time {integer}
        set query-interval {integer}
        set query-timeout {integer}
        set router-alert-check {enable|disable}
    end
next
end
end

```

config router multicast

Parameter	Description	Type	Size	Default
route-threshold	Generate warnings when the number of multicast routes exceeds this number, must not be greater than route-limit.	integer	Minimum value: 1 Maximum value: 2147483647	

Parameter	Description	Type	Size	Default
route-limit	Maximum number of multicast routes.	integer	Minimum value: 1 Maximum value: 2147483647	2147483647
multicast-routing	Enable/disable IP multicast routing.	option	-	disable
Option	Description			
<i>enable</i>	Enable IP multicast routing.			
<i>disable</i>	Disable IP multicast routing.			

config pim-sm-global

Parameter	Description	Type	Size	Default
message-interval	Period of time between sending periodic PIM join/prune messages in seconds .	integer	Minimum value: 1 Maximum value: 65535	60
join-prune-holdtime	Join/prune holdtime .	integer	Minimum value: 1 Maximum value: 65535	210
accept-register-list	Sources allowed to register packets with this Rendezvous Point (RP).	string	Maximum length: 35	
accept-source-list	Sources allowed to send multicast traffic.	string	Maximum length: 35	
bsr-candidate	Enable/disable allowing this router to become a bootstrap router (BSR).	option	-	disable
Option	Description			
<i>enable</i>	Allow this router to function as a BSR.			
<i>disable</i>	Do not allow this router to function as a BSR.			
bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default						
bsr-priority	BSR priority .	integer	Minimum value: 0 Maximum value: 255	0						
bsr-hash	BSR hash length .	integer	Minimum value: 0 Maximum value: 32	10						
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Allow quick refresh packets.</td></tr> <tr> <td><i>disable</i></td><td>Do not allow quick refresh packets.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Allow quick refresh packets.	<i>disable</i>	Do not allow quick refresh packets.
Option	Description									
<i>enable</i>	Allow quick refresh packets.									
<i>disable</i>	Do not allow quick refresh packets.									
cisco-register-checksum	Checksum entire register packet(for old Cisco IOS compatibility).	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>register checksum entire packet.</td></tr> <tr> <td><i>disable</i></td><td>Do not register checksum entire packet.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	register checksum entire packet.	<i>disable</i>	Do not register checksum entire packet.
Option	Description									
<i>enable</i>	register checksum entire packet.									
<i>disable</i>	Do not register checksum entire packet.									
cisco-register-checksum-group	Cisco register checksum only these groups.	string	Maximum length: 35							
cisco-crp-prefix	Enable/disable making candidate RP compatible with old Cisco IOS.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Do not allow sending group prefix of zero.</td></tr> <tr> <td><i>disable</i></td><td>Allow sending group prefix of zero.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Do not allow sending group prefix of zero.	<i>disable</i>	Allow sending group prefix of zero.
Option	Description									
<i>enable</i>	Do not allow sending group prefix of zero.									
<i>disable</i>	Allow sending group prefix of zero.									
cisco-ignore-rp-set-priority	Use only hash for RP selection (compatibility with old Cisco IOS).	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Ignore RP-SET priority value.</td></tr> <tr> <td><i>disable</i></td><td>Do not ignore RP-SET priority value.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Ignore RP-SET priority value.	<i>disable</i>	Do not ignore RP-SET priority value.
Option	Description									
<i>enable</i>	Ignore RP-SET priority value.									
<i>disable</i>	Do not ignore RP-SET priority value.									
register-rp-reachability	Enable/disable check RP is reachable before registering packets.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Check target RP is unicast reachable before registering.		
	<i>disable</i>	Do not check RP unicast reachability.		
register-source	Override source address in register packets.	option	-	disable
	Option	Description		
	<i>disable</i>	Use source address of RPF interface.		
	<i>interface</i>	Use primary IP of an interface.		
	<i>ip-address</i>	Use a local IP address.		
register-source-interface	Override with primary interface address.	string	Maximum length: 15	
register-source-ip	Override with local IP address.	ipv4-address	Not Specified	0.0.0.0
register-suppression	Period of time to honor register-stop message .	integer	Minimum value: 1 Maximum value: 65535	60
null-register-retries	Maximum retries of null register .	integer	Minimum value: 1 Maximum value: 20	1
rp-register-keepalive	Timeout for RP receiving data on .	integer	Minimum value: 1 Maximum value: 65535	185
spt-threshold	Enable/disable switching to source specific trees.	option	-	enable
	Option	Description		
	<i>enable</i>	Switch to Source tree when available.		
	<i>disable</i>	Do not switch to Source tree when available.		
spt-threshold-group	Groups allowed to switch to source tree.	string	Maximum length: 35	
ssm	Enable/disable source specific multicast.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Allow source specific multicast.		
	<i>disable</i>	Do not allow source specific multicast.		
ssm-range	Groups allowed to source specific multicast.	string	Maximum length: 35	
register-rate-limit	Limit of packets/sec per source registered through this RP .	integer	Minimum value: 0 Maximum value: 65535	0

config rp-address

Parameter	Description	Type	Size	Default
ip-address	RP router address.	ipv4-address	Not Specified	0.0.0.0
group	Groups to use this RP.	string	Maximum length: 35	

config interface

Parameter	Description	Type	Size	Default
ttl-threshold	Minimum TTL of multicast packets that will be forwarded .	integer	Minimum value: 1 Maximum value: 255	1
pim-mode	PIM operation mode.	option	-	sparse-mode
	Option	Description		
	<i>sparse-mode</i>	sparse-mode		
	<i>dense-mode</i>	dense-mode		
passive	Enable/disable listening to IGMP but not participating in PIM.	option	-	disable
	Option	Description		
	<i>enable</i>	Listen only.		
	<i>disable</i>	Participate in PIM.		

Parameter	Description	Type	Size	Default
bfd	Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).		
	<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).		
neighbour-filter	Routers acknowledged as neighbor routers.	string	Maximum length: 35	
hello-interval	Interval between sending PIM hello messages .	integer	Minimum value: 1 Maximum value: 65535	30
hello-holdtime	Time before old neighbor information expires .	integer	Minimum value: 1 Maximum value: 65535	
cisco-exclude-genid	Exclude GenID from hello packets (compatibility with old Cisco IOS).	option	-	disable
	Option	Description		
	<i>enable</i>	Do not send GenID.		
	<i>disable</i>	Send GenID according to standard.		
dr-priority	DR election priority.	integer	Minimum value: 1 Maximum value: 4294967295	1
propagation-delay	Delay flooding packets on this interface .	integer	Minimum value: 100 Maximum value: 5000	500
state-refresh-interval	Interval between sending state-refresh packets .	integer	Minimum value: 1 Maximum value: 100	60
rp-candidate	Enable/disable compete to become RP in elections.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Compete for RP elections.		
	<i>disable</i>	Do not compete for RP elections.		
rp-candidate-group	Multicast groups managed by this RP.	string	Maximum length: 35	
rp-candidate-priority	Router's priority as RP.	integer	Minimum value: 0 Maximum value: 255	192
rp-candidate-interval	RP candidate advertisement interval .	integer	Minimum value: 1 Maximum value: 16383	60
multicast-flow	Acceptable source for multicast group.	string	Maximum length: 35	
static-group	Statically set multicast groups to forward out.	string	Maximum length: 35	
rpf-nbr-fail-back	Enable/disable fail back for RPF neighbor query.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fail back for RPF neighbor query.		
	<i>disable</i>	Disable fail back for RPF neighbor query.		
rpf-nbr-fail-back-filter	Filter for fail back RPF neighbors.	string	Maximum length: 35	

config igmp

Parameter	Description	Type	Size	Default
access-group	Groups IGMP hosts are allowed to join.	string	Maximum length: 35	
version	Maximum version of IGMP to support.	option	-	3
	Option	Description		
	3	Version 3 and lower.		
	2	Version 2 and lower.		
	1	Version 1.		

Parameter	Description	Type	Size	Default
immediate-leave-group	Groups to drop membership for immediately after receiving IGMPv2 leave.	string	Maximum length: 35	
last-member-query-interval	Timeout between IGMPv2 leave and removing group .	integer	Minimum value: 1 Maximum value: 65535	1000
last-member-query-count	Number of group specific queries before removing group .	integer	Minimum value: 2 Maximum value: 7	2
query-max-response-time	Maximum time to wait for a IGMP query response .	integer	Minimum value: 1 Maximum value: 25	10
query-interval	Interval between queries to IGMP hosts .	integer	Minimum value: 1 Maximum value: 65535	125
query-timeout	Timeout between queries before becoming querier for network .	integer	Minimum value: 60 Maximum value: 900	255
router-alert-check	Enable/disable require IGMP packets contain router alert option.	option	-	disable
Option	Description			
enable	Require Router Alert option in IGMP packets.			
disable	don't require Router Alert option in IGMP packets			

config router multicast6

Configure IPv6 multicast.

```
config router multicast6
  Description: Configure IPv6 multicast.
  set multicast-routing [enable|disable]
  set multicast-pmtu [enable|disable]
  config interface
    Description: Protocol Independent Multicast (PIM) interfaces.
    edit <name>
      set hello-interval {integer}
      set hello-holddtime {integer}
```

```

        next
    end
    config pim-sm-global
        Description: PIM sparse-mode global settings.
        set register-rate-limit {integer}
    config rp-address
        Description: Statically configured RP addresses.
        edit <id>
            set ip6-address {ip6-address}
        next
    end
end

```

config router multicast6

Parameter	Description	Type	Size	Default
multicast-routing	Enable/disable IPv6 multicast routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv6 multicast routing.		
	<i>disable</i>	Disable IPv6 multicast routing.		
multicast-pmtu	Enable/disable PMTU for IPv6 multicast.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PMTU for IPv6 multicast.		
	<i>disable</i>	Disable PMTU for IPv6 multicast.		

config interface

Parameter	Description	Type	Size	Default
hello-interval	Interval between sending PIM hello messages ..	integer	Minimum value: 1 Maximum value: 65535	30
hello-holdtime	Time before old neighbour information expires .	integer	Minimum value: 1 Maximum value: 65535	

config pim-sm-global

Parameter	Description	Type	Size	Default
register-rate-limit	Limit of packets/sec per source registered through this RP (0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535	0

config rp-address

Parameter	Description	Type	Size	Default
ip6-address	RP router IPv6 address.	ipv6-address	Not Specified	::

config router info

Show routing information.

```
config router info
  Description: Show routing information.
end
```

config router info6

Show IPv6 routing information.

```
config router info6
  Description: Show IPv6 routing information.
end
```

config router auth-path

Configure authentication based routing.

```
config router auth-path
  Description: Configure authentication based routing.
  edit <name>
    set device {string}
    set gateway {ipv4-address}
  next
end
```

config router auth-path

Parameter	Description	Type	Size	Default
device	Outgoing interface.	string	Maximum length: 35	
gateway	Gateway IP address.	ipv4-address	Not Specified	0.0.0.0

config router setting

Configure router settings.

```
config router setting
  Description: Configure router settings.
    set show-filter {string}
    set hostname {string}
end
```

config router setting

Parameter	Description	Type	Size	Default
show-filter	Prefix-list as filter for showing routes.	string	Maximum length: 35	
hostname	Hostname for this virtual domain router.	string	Maximum length: 14	

config router bfd

Configure BFD.

```
config router bfd
  Description: Configure BFD.
    config neighbor
      Description: neighbor
        edit <ip>
          set interface {string}
        next
      end
    end
end
```

config neighbor

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	

config router bfd6

Configure IPv6 BFD.

```
config router bfd6
    Description: Configure IPv6 BFD.
    config neighbor
        Description: Configure neighbor of IPv6 BFD.
        edit <ip6-address>
            set interface {string}
        next
    end
end
```

config neighbor

Parameter	Description	Type	Size	Default
interface	Interface to the BFD neighbor.	string	Maximum length: 15	

sctp-filter

This section includes syntax for the following commands:

- [config sctp-filter profile on page 743](#)

config sctp-filter profile

Configure SCTP filter profiles.

```
config sctp-filter profile
  Description: Configure SCTP filter profiles.
  edit <name>
    set comment {var-string}
    config ppid-filters
      Description: PPID filters list.
      edit <id>
        set ppid {integer}
        set action [pass|reset|...]
        set comment {var-string}
      next
    end
  next
end
```

config sctp-filter profile

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

config ppid-filters

Parameter	Description	Type	Size	Default
ppid	Payload protocol identifier.	integer	Minimum value: 0 Maximum value: 4294967295	
action	Action taken when PPID is matched.	option	-	reset

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Pass data chunk.		
	<i>reset</i>	Reset SCTP session.		
	<i>replace</i>	Replace data chunk.		
comment	Comment.	var-string	Maximum length: 255	

ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 745](#)

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
block	SSH blocking 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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
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

Parameter	Description	Type	Size	Default
	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.		

switch-controller

This section includes syntax for the following commands:

- [config switch-controller fortilink-settings on page 750](#)
- [config switch-controller auto-config policy on page 775](#)
- [config switch-controller switch-group on page 816](#)
- [config switch-controller qos queue-policy on page 770](#)
- [config switch-controller system on page 823](#)
- [config switch-controller snmp-user on page 834](#)
- [config switch-controller lldp-profile on page 762](#)
- [config switch-controller dynamic-port-policy on page 782](#)
- [config switch-controller flow-tracking on page 828](#)
- [config switch-controller security-policy 802-1X on page 753](#)
- [config switch-controller switch-profile on page 779](#)
- [config switch-controller vlan-policy on page 781](#)
- [config switch-controller qos ip-dscp-map on page 769](#)
- [config switch-controller stp-settings on page 817](#)
- [config switch-controller qos qos-policy on page 773](#)
- [config switch-controller security-policy local-access on page 756](#)
- [config switch-controller mac-policy on page 840](#)
- [config switch-controller storm-control-policy on page 773](#)
- [config switch-controller quarantine on page 826](#)
- [config switch-controller 802-1X-settings on page 752](#)
- [config switch-controller virtual-port-pool on page 780](#)
- [config switch-controller snmp-community on page 832](#)
- [config switch-controller traffic-sniffer on page 836](#)
- [config switch-controller snmp-sysinfo on page 830](#)
- [config switch-controller auto-config custom on page 776](#)
- [config switch-controller managed-switch on page 784](#)
- [config switch-controller stp-instance on page 818](#)
- [config switch-controller switch-log on page 824](#)
- [config switch-controller ptp settings on page 780](#)
- [config switch-controller storm-control on page 818](#)
- [config switch-controller igmp-snooping on page 825](#)
- [config switch-controller ptp policy on page 781](#)
- [config switch-controller location on page 757](#)
- [config switch-controller sflow on page 826](#)
- [config switch-controller network-monitor-settings on page 827](#)
- [config switch-controller global on page 819](#)
- [config switch-controller remote-log on page 837](#)
- [config switch-controller qos dot1p-map on page 765](#)
- [config switch-controller initial-config template on page 776](#)

- [config switch-controller initial-config vlans](#) on page 778
- [config switch-controller traffic-policy](#) on page 749
- [config switch-controller snmp-trap-threshold](#) on page 831
- [config switch-controller lldp-settings](#) on page 761
- [config switch-controller custom-command](#) on page 779
- [config switch-controller switch-interface-tag](#) on page 752
- [config switch-controller auto-config default](#) on page 775

config switch-controller traffic-policy

Configure FortiSwitch traffic policy.

```
config switch-controller traffic-policy
  Description: Configure FortiSwitch traffic policy.
  edit <name>
    set description {string}
    set policer-status [enable|disable]
    set guaranteed-bandwidth {integer}
    set guaranteed-burst {integer}
    set maximum-burst {integer}
    set type [ingress|egress]
    set cos-queue {integer}
  next
end
```

config switch-controller traffic-policy

Parameter	Description	Type	Size	Default				
description	Description of the traffic policy.	string	Maximum length: 63					
	Option	Description						
policer-status	Enable/disable policer config on the traffic policy.	option	-	enable				
		<table border="1"> <tr> <td><i>enable</i></td> <td>Enable policer config on the traffic policy.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable policer config on the traffic policy.</td> </tr> </table>			<i>enable</i>	Enable policer config on the traffic policy.	<i>disable</i>	Disable policer config on the traffic policy.
<i>enable</i>	Enable policer config on the traffic policy.							
<i>disable</i>	Disable policer config on the traffic policy.							
guaranteed-bandwidth	Guaranteed bandwidth in kbps (max value = 524287000).	integer	Minimum value: 0 Maximum value: 524287000	10000				
guaranteed-burst	Guaranteed burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	45000				

Parameter	Description	Type	Size	Default
maximum-burst	Maximum burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	67500
type	Configure type of policy(ingress/egress).	option	-	ingress
Option		Description		
		<i>ingress</i> Ingress policy.		
		<i>egress</i> Egress policy.		
cos-queue	COS queue, or unset to disable.	integer	Minimum value: 0 Maximum value: 7	

config switch-controller fortilink-settings

Configure integrated FortiLink settings for FortiSwitch.

```
config switch-controller fortilink-settings
  Description: Configure integrated FortiLink settings for FortiSwitch.
  edit <name>
    set inactive-timer {integer}
    set link-down-flush [disable|enable]
    config nac-ports
      Description: NAC specific configuration.
      set onboarding-vlan {string}
      set bounce-nac-port [disable|enable]
      set lan-segment [enabled|disabled]
      set nac-lan-interface {string}
      set nac-segment-vlans <vlan-name1>, <vlan-name2>, ...
      set parent-key {string}
      set member-change {integer}
    end
  next
end
```

config switch-controller fortilink-settings

Parameter	Description	Type	Size	Default
inactive-timer	Time interval(minutes) to be included in the inactive devices expiry calculation (mac age-out + inactive-time + periodic scan interval).	integer	Minimum value: 1 Maximum value: 1440	15

Parameter	Description	Type	Size	Default
link-down-flush	Clear NAC and dynamic devices on switch ports on link down event.	option	-	enable
Parameter	Description	Type	Size	Default
Option	Description			
<i>disable</i>				Disable clearing NAC and dynamic devices on a switch port when link down event happens.
<i>enable</i>				Enable clearing NAC and dynamic devices on a switch port when link down event happens.

config nac-ports

Parameter	Description	Type	Size	Default
onboarding-vlan	Default NAC Onboarding VLAN when NAC devices are discovered.	string	Maximum length: 15	
bounce-nac-port	Enable/disable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured on the port. Helps to re-initiate the DHCP process for a device.	option	-	enable
Parameter	Description	Type	Size	Default
Option	Description			
<i>disable</i>				Disable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.
<i>enable</i>				Enable bouncing (administratively bring the link down, up) of a switch port when NAC mode is configured.
lan-segment	Enable/disable LAN segment feature on the FortiLink interface.	option	-	disabled
Parameter	Description	Type	Size	Default
Option	Description			
<i>enabled</i>				Enable lan-segment on this interface.
<i>disabled</i>				Disable lan-segment on this interface.
nac-lan-interface	Configure NAC LAN interface.	string	Maximum length: 15	
nac-segment-vlans <vlan-name>	Configure NAC segment VLANs. VLAN interface name.	string	Maximum length: 79	
parent-key	Parent key name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
member-change	Member change flag.	integer	Minimum value: 0 Maximum value: 255	0

config switch-controller switch-interface-tag

Configure switch object tags.

```
config switch-controller switch-interface-tag
  Description: Configure switch object tags.
  edit <name>
  next
end
```

config switch-controller 802-1X-settings

Configure global 802.1X settings.

```
config switch-controller 802-1X-settings
  Description: Configure global 802.1X settings.
  set link-down-auth {set-unauth|no-action}
  set reauth-period {integer}
  set max-reauth-attempt {integer}
  set tx-period {integer}
end
```

config switch-controller 802-1X-settings

Parameter	Description	Type	Size	Default
link-down-auth	Interface-reauthentication state to set if a link is down.	option	-	set-unauth
Option	Description			
<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.			
<i>no-action</i>	Interface reauthentication is not needed.			
reauth-period	Period of time to allow for reauthentication .	integer	Minimum value: 0 Maximum value: 1440	60
max-reauth-attempt	Maximum number of authentication attempts .	integer	Minimum value: 0 Maximum value: 15	3

Parameter	Description	Type	Size	Default
tx-period	802.1X Tx period .	integer	Minimum value: 4 Maximum value: 60	30

config switch-controller security-policy 802-1X

Configure 802.1x MAC Authentication Bypass (MAB) policies.

```
config switch-controller security-policy 802-1X
  Description: Configure 802.1x MAC Authentication Bypass (MAB) policies.
  edit <name>
    set security-mode [802.1X|802.1X-mac-based]
    set user-group <name1>, <name2>, ...
    set mac-auth-bypass [disable|enable]
    set open-auth [disable|enable]
    set eap-passthru [disable|enable]
    set eap-auto-untagged-vlans [disable|enable]
    set guest-vlan [disable|enable]
    set guest-vlan-id {string}
    set guest-auth-delay {integer}
    set auth-fail-vlan [disable|enable]
    set auth-fail-vlan-id {string}
    set framevid-apply [disable|enable]
    set radius-timeout-overwrite [disable|enable]
    set policy-type {option}
    set authserver-timeout-period {integer}
    set authserver-timeout-vlan [disable|enable]
    set authserver-timeout-vlanid {string}
  next
end
```

config switch-controller security-policy 802-1X

Parameter	Description	Type	Size	Default
security-mode	Port or MAC based 802.1X security mode.	option	-	802.1X
Option	Description			
802.1X	802.1X port based authentication.			
802.1X-mac-based	802.1X MAC based authentication.			
user-group <name>	Name of user-group to assign to this MAC Authentication Bypass (MAB) policy. Group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
mac-auth-bypass	Enable/disable MAB for this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable MAB.		
	<i>enable</i>	Enable MAB.		
open-auth	Enable/disable open authentication for this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable open authentication.		
	<i>enable</i>	Enable open authentication.		
eap-passthru	Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for more flexible authentication.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable EAP pass-through mode on this interface.		
	<i>enable</i>	Enable EAP pass-through mode on this interface.		
eap-auto-untagged-vlans	Enable/disable automatic inclusion of untagged VLANs.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable automatic inclusion of untagged VLANs.		
	<i>enable</i>	Enable automatic inclusion of untagged VLANs.		
guest-vlan	Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable guest VLAN on this interface.		
	<i>enable</i>	Enable guest VLAN on this interface.		
guest-vlan-id	Guest VLAN name.	string	Maximum length: 15	
guest-auth-delay	Guest authentication delay .	integer	Minimum value: 1 Maximum value: 900	30

Parameter	Description	Type	Size	Default
auth-fail-vlan	Enable to allow limited access to clients that cannot authenticate.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable authentication fail VLAN on this interface.		
	<i>enable</i>	Enable authentication fail VLAN on this interface.		
auth-fail-vlan-id	VLAN ID on which authentication failed.	string	Maximum length: 15	
framevid-apply	Enable/disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
	<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
radius-timeout-overwrite	Enable to override the global RADIUS session timeout.	option	-	disable
	Option	Description		
	<i>disable</i>	Override the global RADIUS session timeout.		
	<i>enable</i>	Use the global RADIUS session timeout.		
policy-type	Policy type.	option	-	802.1X
	Option	Description		
	<i>802.1X</i>	802.1X security policy.		
authserver-timeout-period	Authentication server timeout period .	integer	Minimum value: 3 Maximum value: 15	3
authserver-timeout-vlan	Enable/disable the authentication server timeout VLAN to allow limited access when RADIUS is unavailable.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable authentication server timeout VLAN on this interface.		
	<i>enable</i>	Enable authentication server timeout VLAN on this interface.		

Parameter	Description	Type	Size	Default
authserver-timeout-vlanid	Authentication server timeout VLAN name.	string	Maximum length: 15	

config switch-controller security-policy local-access

Configure allowaccess list for mgmt and internal interfaces on managed FortiSwitch.

```
config switch-controller security-policy local-access
  Description: Configure allowaccess list for mgmt and internal interfaces on managed
    FortiSwitch.
  edit <name>
    set mgmt-allowaccess {option1}, {option2}, ...
    set internal-allowaccess {option1}, {option2}, ...
  next
end
```

config switch-controller security-policy local-access

Parameter	Description	Type	Size	Default
mgmt-allowaccess	Allowed access on the switch management interface.	option	-	https ping ssh
Option		Description		
<i>https</i>		HTTPS access.		
<i>ping</i>		PING access.		
<i>ssh</i>		SSH access.		
<i>snmp</i>		SNMP access.		
<i>http</i>		HTTP access.		
<i>telnet</i>		TELNET access.		
<i>radius-acct</i>		RADIUS accounting access.		
internal-allowaccess	Allowed access on the switch internal interface.	option	-	https ping ssh
Option		Description		
<i>https</i>		HTTPS access.		
<i>ping</i>		PING access.		
<i>ssh</i>		SSH access.		

Parameter	Description	Type	Size	Default
Option	Description			
<i>snmp</i>	SNMP access.			
<i>http</i>	HTTP access.			
<i>telnet</i>	TELNET access.			
<i>radius-acct</i>	RADIUS accounting access.			

config switch-controller location

Configure FortiSwitch location services.

```
config switch-controller location
  Description: Configure FortiSwitch location services.
  edit <name>
    config address-civic
      Description: Configure location civic address.
      set additional {string}
      set additional-code {string}
      set block {string}
      set branch-road {string}
      set building {string}
      set city {string}
      set city-division {string}
      set country {string}
      set country-subdivision {string}
      set county {string}
      set direction {string}
      set floor {string}
      set landmark {string}
      set language {string}
      set name {string}
      set number {string}
      set number-suffix {string}
      set place-type {string}
      set post-office-box {string}
      set postal-community {string}
      set primary-road {string}
      set road-section {string}
      set room {string}
      set script {string}
      set seat {string}
      set street {string}
      set street-name-post-mod {string}
      set street-name-pre-mod {string}
      set street-suffix {string}
      set sub-branch-road {string}
      set trailing-str-suffix {string}
      set unit {string}
      set zip {string}
      set parent-key {string}
  end
```

```

config coordinates
    Description: Configure location GPS coordinates.
    set altitude {string}
    set altitude-unit [m|f]
    set datum [WGS84|NAD83|...]
    set latitude {string}
    set longitude {string}
    set parent-key {string}
end
config elin-number
    Description: Configure location ELIN number.
    set elin-num {string}
    set parent-key {string}
end
next
end

```

config address-civic

Parameter	Description	Type	Size	Default
additional	Location additional details.	string	Maximum length: 47	
additional-code	Location additional code details.	string	Maximum length: 47	
block	Location block details.	string	Maximum length: 47	
branch-road	Location branch road details.	string	Maximum length: 47	
building	Location building details.	string	Maximum length: 47	
city	Location city details.	string	Maximum length: 47	
city-division	Location city division details.	string	Maximum length: 47	
country	The two-letter ISO 3166 country code in capital ASCII letters eg. US, CA, DK, DE.	string	Maximum length: 47	
country-subdivision	National subdivisions (state, canton, region, province, or prefecture).	string	Maximum length: 47	
county	County, parish, gun (JP), or district (IN).	string	Maximum length: 47	
direction	Leading street direction.	string	Maximum length: 47	
floor	Floor.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
landmark	Landmark or vanity address.	string	Maximum length: 47	
language	Language.	string	Maximum length: 47	
name	Name (residence and office occupant).	string	Maximum length: 47	
number	House number.	string	Maximum length: 47	
number-suffix	House number suffix.	string	Maximum length: 47	
place-type	Placetype.	string	Maximum length: 47	
post-office-box	Post office box (P.O. box).	string	Maximum length: 47	
postal-community	Postal community name.	string	Maximum length: 47	
primary-road	Primary road name.	string	Maximum length: 47	
road-section	Road section.	string	Maximum length: 47	
room	Room number.	string	Maximum length: 47	
script	Script used to present the address information.	string	Maximum length: 47	
seat	Seat number.	string	Maximum length: 47	
street	Street.	string	Maximum length: 47	
street-name-post-mod	Street name post modifier.	string	Maximum length: 47	
street-name-pre-mod	Street name pre modifier.	string	Maximum length: 47	
street-suffix	Street suffix.	string	Maximum length: 47	
sub-branch-road	Sub branch road name.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
trailing-str-suffix	Trailing street suffix.	string	Maximum length: 47	
unit	Unit (apartment, suite).	string	Maximum length: 47	
zip	Postal/zip code.	string	Maximum length: 47	
parent-key	Parent key name.	string	Maximum length: 63	

config coordinates

Parameter	Description	Type	Size	Default
altitude	+/- Floating point no. eg. 117.47.	string	Maximum length: 15	
altitude-unit	m (meters), f (floors).	option	-	m
Option		Description		
		<i>m</i>	set altitude unit meters	
		<i>f</i>	set altitude unit floors	
datum	WGS84, NAD83, NAD83/MLLW.	option	-	WGS84
Option		Description		
		<i>WGS84</i>	set coordinates datum WGS84	
		<i>NAD83</i>	set coordinates datum NAD83	
		<i>NAD83/MLLW</i>	set coordinates datum NAD83/MLLW	
latitude	Floating point start with (+/-) or end with (N or S) eg. +/-16.67 or 16.67N.	string	Maximum length: 15	
longitude	Floating point start with (+/-) or end with (E or W) eg. +/-26.789 or 26.789E.	string	Maximum length: 15	
parent-key	Parent key name.	string	Maximum length: 63	

config elin-number

Parameter	Description	Type	Size	Default
elin-num	Configure ELIN callback number.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
parent-key	Parent key name.	string	Maximum length: 63	

config switch-controller lldp-settings

Configure FortiSwitch LLDP settings.

```
config switch-controller lldp-settings
  Description: Configure FortiSwitch LLDP settings.
  set tx-hold {integer}
  set tx-interval {integer}
  set fast-start-interval {integer}
  set management-interface [internal|mgmt]
  set device-detection [disable|enable]
end
```

config switch-controller lldp-settings

Parameter	Description	Type	Size	Default
tx-hold	Number of tx-intervals before local LLDP data expires . Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 1 Maximum value: 16	4
tx-interval	Frequency of LLDP PDU transmission from FortiSwitch . Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 5 Maximum value: 4095	30
fast-start-interval	Frequency of LLDP PDU transmission from FortiSwitch for the first 4 packets when the link is up .	integer	Minimum value: 0 Maximum value: 255	2
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	option	-	internal
	Option	Description		
	<i>internal</i>	Use internal interface.		
	<i>mgmt</i>	Use management interface.		
device-detection	Enable/disable dynamic detection of LLDP neighbor devices for VLAN assignment.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable dynamic detection of LLDP neighbor devices.		
	<i>enable</i>	Enable dynamic detection of LLDP neighbor devices.		

config switch-controller lldp-profile

Configure FortiSwitch LLDP profiles.

```

config switch-controller lldp-profile
    Description: Configure FortiSwitch LLDP profiles.
    edit <name>
        set med-tlvs {option1}, {option2}, ...
        set 802 1-tlvs {option1}, {option2}, ...
        set 802 3-tlvs {option1}, {option2}, ...
        set auto-isl [disable|enable]
        set auto-isl-hello-timer {integer}
        set auto-isl-receive-timeout {integer}
        set auto-isl-port-group {integer}
        set auto-mLAG-ICL [disable|enable]
        config med-network-policy
            Description: Configuration method to edit Media Endpoint Discovery (MED) network
                         policy type-length-value (TLV) categories.
            edit <name>
                set status [disable|enable]
                set vlan-intf {string}
                set assign-vlan [disable|enable]
                set priority {integer}
                set dscp {integer}
            next
        end
        config med-location-service
            Description: Configuration method to edit Media Endpoint Discovery (MED) location
                         service type-length-value (TLV) categories.
            edit <name>
                set status [disable|enable]
                set sys-location-id {string}
            next
        end
        config custom-tlvs
            Description: Configuration method to edit custom TLV entries.
            edit <name>
                set oui {user}
                set subtype {integer}
                set information-string {user}
            next
        end
    next
end

```

config switch-controller lldp-profile

Parameter	Description	Type	Size	Default
med-tlvs	Transmitted LLDP-MED TLVs (type-length-value descriptions).	option	-	
	Option	Description		
	<i>inventory-management</i>	Inventory management TLVs.		
	<i>network-policy</i>	Network policy TLVs.		
	<i>power-management</i>	Power manangement TLVs.		
	<i>location-identification</i>	Location identificaion TLVs.		
802.1-tlvs	Transmitted IEEE 802.1 TLVs.	option	-	
	Option	Description		
	<i>port-vlan-id</i>	Port native VLAN TLV.		
802.3-tlvs	Transmitted IEEE 802.3 TLVs.	option	-	
	Option	Description		
	<i>max-frame-size</i>	Maximum frame size TLV.		
	<i>power-negotiation</i>	PoE+ classification TLV.		
auto-isl	Enable/disable auto inter-switch LAG.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable automatic MLAG inter chassis link.		
	<i>enable</i>	Enable automatic MLAG inter chassis link.		
auto-isl-hello-timer	Auto inter-switch LAG hello timer duration .	integer	Minimum value: 1 Maximum value: 30	3
auto-isl-receive-timeout	Auto inter-switch LAG timeout if no response is received .	integer	Minimum value: 0 Maximum value: 90	60

Parameter	Description	Type	Size	Default
auto-isl-port-group	Auto inter-switch LAG port group ID .	integer	Minimum value: 0 Maximum value: 9	0
auto-mclag-icl	Enable/disable MCLAG inter chassis link.	option	-	disable
Option		Description		
		<i>disable</i> Disable auto inter-switch-LAG.		
		<i>enable</i> Enable auto inter-switch-LAG.		

config med-network-policy

Parameter	Description	Type	Size	Default
status	Enable or disable this TLV.	option	-	disable
Option		Description		
		<i>disable</i> Do not transmit this network policy TLV.		
		<i>enable</i> Transmit this TLV if a VLAN has been added to the port.		
vlan-intf	VLAN interface to advertise; if configured on port.	string	Maximum length: 15	
assign-vlan	Enable/disable VLAN assignment when this profile is applied on managed FortiSwitch port.	option	-	disable
Option		Description		
		<i>disable</i> Disable VLAN assignment when this profile is applied on port.		
		<i>enable</i> Enable VLAN assignment when this profile is applied on port.		
priority	Advertised Layer 2 priority .	integer	Minimum value: 0 Maximum value: 7	0
dscp	Advertised Differentiated Services Code Point (DSCP) value, a packet header value indicating the level of service requested for traffic, such as high priority or best effort delivery.	integer	Minimum value: 0 Maximum value: 63	0

config med-location-service

Parameter	Description	Type	Size	Default
status	Enable or disable this TLV.	option	-	disable
Parameter	Description	Type	Size	Default
sys-location-id	Location service ID.	string	Maximum length: 63	
Parameter	Description	Type	Size	Default

config custom-tlvs

Parameter	Description	Type	Size	Default
oui	Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.	user	Not Specified	000000
subtype	Organizationally defined subtype .	integer	Minimum value: 0 Maximum value: 255	0
information-string	Organizationally defined information string .	user	Not Specified	

config switch-controller qos dot1p-map

Configure FortiSwitch QoS 802.1p.

```
config switch-controller qos dot1p-map
  Description: Configure FortiSwitch QoS 802.1p.
  edit <name>
    set description {string}
    set egress-pri-tagging [disable|enable]
    set priority-0 [queue-0|queue-1|...]
    set priority-1 [queue-0|queue-1|...]
    set priority-2 [queue-0|queue-1|...]
    set priority-3 [queue-0|queue-1|...]
    set priority-4 [queue-0|queue-1|...]
    set priority-5 [queue-0|queue-1|...]
    set priority-6 [queue-0|queue-1|...]
    set priority-7 [queue-0|queue-1|...]
  next
end
```

config switch-controller qos dot1p-map

Parameter	Description	Type	Size	Default
description	Description of the 802.1p name.	string	Maximum length: 63	
egress-pri-tagging	Enable/disable egress priority-tag frame.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable egress priority tagging.		
	<i>enable</i>	Enable egress priority tagging.		
priority-0	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-1	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-2	COS queue mapped to dot1p priority number.	option	-	queue-0

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-3	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-4	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		

Parameter	Description	Type	Size	Default																		
priority-5	COS queue mapped to dot1p priority number.	option	-	queue-0																		
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>queue-0</i></td><td>COS queue 0 (lowest priority).</td></tr> <tr> <td><i>queue-1</i></td><td>COS queue 1.</td></tr> <tr> <td><i>queue-2</i></td><td>COS queue 2.</td></tr> <tr> <td><i>queue-3</i></td><td>COS queue 3.</td></tr> <tr> <td><i>queue-4</i></td><td>COS queue 4.</td></tr> <tr> <td><i>queue-5</i></td><td>COS queue 5.</td></tr> <tr> <td><i>queue-6</i></td><td>COS queue 6.</td></tr> <tr> <td><i>queue-7</i></td><td>COS queue 7 (highest priority).</td></tr> </tbody> </table>					Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-6	COS queue mapped to dot1p priority number.	option	-	queue-0																		
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>queue-0</i></td><td>COS queue 0 (lowest priority).</td></tr> <tr> <td><i>queue-1</i></td><td>COS queue 1.</td></tr> <tr> <td><i>queue-2</i></td><td>COS queue 2.</td></tr> <tr> <td><i>queue-3</i></td><td>COS queue 3.</td></tr> <tr> <td><i>queue-4</i></td><td>COS queue 4.</td></tr> <tr> <td><i>queue-5</i></td><td>COS queue 5.</td></tr> <tr> <td><i>queue-6</i></td><td>COS queue 6.</td></tr> <tr> <td><i>queue-7</i></td><td>COS queue 7 (highest priority).</td></tr> </tbody> </table>					Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					
priority-7	COS queue mapped to dot1p priority number.	option	-	queue-0																		
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>queue-0</i></td><td>COS queue 0 (lowest priority).</td></tr> <tr> <td><i>queue-1</i></td><td>COS queue 1.</td></tr> <tr> <td><i>queue-2</i></td><td>COS queue 2.</td></tr> <tr> <td><i>queue-3</i></td><td>COS queue 3.</td></tr> <tr> <td><i>queue-4</i></td><td>COS queue 4.</td></tr> <tr> <td><i>queue-5</i></td><td>COS queue 5.</td></tr> <tr> <td><i>queue-6</i></td><td>COS queue 6.</td></tr> <tr> <td><i>queue-7</i></td><td>COS queue 7 (highest priority).</td></tr> </tbody> </table>					Option	Description	<i>queue-0</i>	COS queue 0 (lowest priority).	<i>queue-1</i>	COS queue 1.	<i>queue-2</i>	COS queue 2.	<i>queue-3</i>	COS queue 3.	<i>queue-4</i>	COS queue 4.	<i>queue-5</i>	COS queue 5.	<i>queue-6</i>	COS queue 6.	<i>queue-7</i>	COS queue 7 (highest priority).
Option	Description																					
<i>queue-0</i>	COS queue 0 (lowest priority).																					
<i>queue-1</i>	COS queue 1.																					
<i>queue-2</i>	COS queue 2.																					
<i>queue-3</i>	COS queue 3.																					
<i>queue-4</i>	COS queue 4.																					
<i>queue-5</i>	COS queue 5.																					
<i>queue-6</i>	COS queue 6.																					
<i>queue-7</i>	COS queue 7 (highest priority).																					

config switch-controller qos ip-dscp-map

Configure FortiSwitch QoS IP precedence/DSCP.

```
config switch-controller qos ip-dscp-map
    Description: Configure FortiSwitch QoS IP precedence/DSCP.
    edit <name>
        set description {string}
        config map
            Description: Maps between IP-DSCP value to COS queue.
            edit <name>
                set cos-queue {integer}
                set diffserv {option1}, {option2}, ...
                set ip-precedence {option1}, {option2}, ...
                set value {user}
            next
        end
    next
end
```

config switch-controller qos ip-dscp-map

Parameter	Description	Type	Size	Default
description	Description of the ip-dscp map name.	string	Maximum length: 63	

config map

Parameter	Description	Type	Size	Default
cos-queue	COS queue number.	integer	Minimum value: 0 Maximum value: 7	0
diffserv	Differentiated service.	option	-	

Option	Description
CS0	DSCP CS0.
CS1	DSCP CS1.
AF11	DSCP AF11.
AF12	DSCP AF12.
AF13	DSCP AF13.
CS2	DSCP CS2.
AF21	DSCP AF21.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>AF22</i>	DSCP AF22.		
	<i>AF23</i>	DSCP AF23.		
	<i>CS3</i>	DSCP CS3.		
	<i>AF31</i>	DSCP AF31.		
	<i>AF32</i>	DSCP AF32.		
	<i>AF33</i>	DSCP AF33.		
	<i>CS4</i>	DSCP CS4.		
	<i>AF41</i>	DSCP AF41.		
	<i>AF42</i>	DSCP AF42.		
	<i>AF43</i>	DSCP AF43.		
	<i>CS5</i>	DSCP CS5.		
	<i>EF</i>	DSCP EF.		
	<i>CS6</i>	DSCP CS6.		
	<i>CS7</i>	DSCP CS7.		
ip-precedence	IP Precedence.	option	-	
	Option	Description		
	<i>network-control</i>	Network control.		
	<i>internetwork-control</i>	Internetwork control.		
	<i>critic-ecp</i>	Critic ECP.		
	<i>flashoverride</i>	Flash override.		
	<i>flash</i>	Flash.		
	<i>immediate</i>	Immediate.		
	<i>priority</i>	Priority.		
	<i>routine</i>	Routine.		
value	Raw values of DSCP .	user	Not Specified	

config switch-controller qos queue-policy

Configure FortiSwitch QoS egress queue policy.

```

config switch-controller qos queue-policy
Description: Configure FortiSwitch QoS egress queue policy.
edit <name>
    set schedule [strict|round-robin|...]
    set rate-by [kbps|percent]
    config cos-queue
        Description: COS queue configuration.
        edit <name>
            set description {string}
            set min-rate {integer}
            set max-rate {integer}
            set min-rate-percent {integer}
            set max-rate-percent {integer}
            set drop-policy [taildrop|weighted-random-early-detection]
            set ecn [disable|enable]
            set weight {integer}
        next
    end
next
end

```

config switch-controller qos queue-policy

Parameter	Description		Type	Size	Default								
schedule	COS queue scheduling.		option	-	round-robin								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>strict</i></td> <td>Strict scheduling (queue7: highest priority, queue0: lowest priority).</td> </tr> <tr> <td><i>round-robin</i></td> <td>Round robin scheduling.</td> </tr> <tr> <td><i>weighted</i></td> <td>Weighted round robin scheduling.</td> </tr> </tbody> </table>		Option	Description	<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).	<i>round-robin</i>	Round robin scheduling.	<i>weighted</i>	Weighted round robin scheduling.			
Option	Description												
<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).												
<i>round-robin</i>	Round robin scheduling.												
<i>weighted</i>	Weighted round robin scheduling.												
rate-by	COS queue rate by kbps or percent.		option	-	kbps								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>kbps</i></td> <td>Rate by kbps.</td> </tr> <tr> <td><i>percent</i></td> <td>Rate by percent.</td> </tr> </tbody> </table>		Option	Description	<i>kbps</i>	Rate by kbps.	<i>percent</i>	Rate by percent.					
Option	Description												
<i>kbps</i>	Rate by kbps.												
<i>percent</i>	Rate by percent.												

config cos-queue

Parameter	Description		Type	Size	Default
description	Description of the COS queue.		string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
min-rate	Minimum rate .	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-rate	Maximum rate .	integer	Minimum value: 0 Maximum value: 4294967295	0						
min-rate-percent	Minimum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-rate-percent	Maximum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0						
drop-policy	COS queue drop policy.	option	-	taildrop						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>taildrop</i></td><td>Taildrop policy.</td></tr> <tr> <td><i>weighted-random-early-detection</i></td><td>Weighted random early detection drop policy.</td></tr> </tbody> </table>					Option	Description	<i>taildrop</i>	Taildrop policy.	<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.
Option	Description									
<i>taildrop</i>	Taildrop policy.									
<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.									
ecn	Enable/disable ECN packet marking to drop eligible packets.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable ECN packet marking to drop eligible packets.</td></tr> <tr> <td><i>enable</i></td><td>Enable ECN packet marking to drop eligible packets.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable ECN packet marking to drop eligible packets.	<i>enable</i>	Enable ECN packet marking to drop eligible packets.
Option	Description									
<i>disable</i>	Disable ECN packet marking to drop eligible packets.									
<i>enable</i>	Enable ECN packet marking to drop eligible packets.									
weight	Weight of weighted round robin scheduling.	integer	Minimum value: 0 Maximum value: 4294967295	1						

config switch-controller qos qos-policy

Configure FortiSwitch QoS policy.

```
config switch-controller qos qos-policy
    Description: Configure FortiSwitch QoS policy.
    edit <name>
        set default-cos {integer}
        set trust-dot1p-map {string}
        set trust-ip-dscp-map {string}
        set queue-policy {string}
    next
end
```

config switch-controller qos qos-policy

Parameter	Description	Type	Size	Default
default-cos	Default cos queue for untagged packets.	integer	Minimum value: 0 Maximum value: 7	0
trust-dot1p-map	QoS trust 802.1p map.	string	Maximum length: 63	
trust-ip-dscp-map	QoS trust ip dscp map.	string	Maximum length: 63	
queue-policy	QoS egress queue policy.	string	Maximum length: 63	default

config switch-controller storm-control-policy

Configure FortiSwitch storm control policy to be applied on managed-switch ports.

```
config switch-controller storm-control-policy
    Description: Configure FortiSwitch storm control policy to be applied on managed-switch
                 ports.
    edit <name>
        set description {string}
        set storm-control-mode [global|override|...]
        set rate {integer}
        set unknown-unicast [enable|disable]
        set unknown-multicast [enable|disable]
        set broadcast [enable|disable]
    next
end
```

config switch-controller storm-control-policy

Parameter	Description	Type	Size	Default
description	Description of the storm control policy.	string	Maximum length: 63	
	Option	Description		
storm-control-mode		<p><i>global</i> Apply Global or switch level storm control configuration.</p> <p><i>override</i> Override global and switch level storm control to use port level configuration.</p> <p><i>disabled</i> Disable storm control on the port entirely overriding global and switch level storm control.</p>		
rate	Threshold rate in packets per second at which storm traffic is controlled in override mode .	integer	Minimum value: 0 Maximum value: 10000000	500
unknown-unicast	Enable/disable storm control to drop/allow unknown unicast traffic in override mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.		
	<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.		
unknown-multicast	Enable/disable storm control to drop/allow unknown multicast traffic in override mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.		
	<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.		
broadcast	Enable/disable storm control to drop/allow broadcast traffic in override mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.		
	<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.		

config switch-controller auto-config policy

Policy definitions which can define the behavior on auto configured interfaces.

```
config switch-controller auto-config policy
  Description: Policy definitions which can define the behavior on auto configured interfaces.
  edit <name>
    set qos-policy {string}
    set storm-control-policy {string}
    set poe-status [enable|disable]
    set igmp-flood-report [enable|disable]
    set igmp-flood-traffic [enable|disable]
  next
end
```

config switch-controller auto-config policy

Parameter	Description	Type	Size	Default
qos-policy	Auto-Config QoS policy.	string	Maximum length: 63	default
storm-control-policy	Auto-Config storm control policy.	string	Maximum length: 63	auto-config
poe-status	Enable/disable PoE status.	option	-	enable
Option	Description			
enable	Enable PoE status.			
disable	Disable PoE status.			
igmp-flood-report	Enable/disable IGMP flood report.	option	-	disable
Option	Description			
enable	Enable IGMP flood report.			
disable	Disable IGMP flood report.			
igmp-flood-traffic	Enable/disable IGMP flood traffic.	option	-	disable
Option	Description			
enable	Enable IGMP flood traffic.			
disable	Disable IGMP flood traffic.			

config switch-controller auto-config default

Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.

```

config switch-controller auto-config default
    Description: Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.
    set fgt-policy {string}
    set isl-policy {string}
    set icl-policy {string}
end

```

config switch-controller auto-config default

Parameter	Description	Type	Size	Default
fgt-policy	Default FortiLink auto-config policy.	string	Maximum length: 63	default
isl-policy	Default ISL auto-config policy.	string	Maximum length: 63	default
icl-policy	Default ICL auto-config policy.	string	Maximum length: 63	default-icl

config switch-controller auto-config custom

Policies which can override the 'default' for specific ISL/ICL/FortiLink interface.

```

config switch-controller auto-config custom
    Description: Policies which can override the 'default' for specific ISL/ICL/FortiLink
                 interface.
    edit <name>
        config switch-binding
            Description: Switch binding list.
            edit <switch-id>
                set policy {string}
            next
        end
    next
end

```

config switch-binding

Parameter	Description	Type	Size	Default
policy	Custom auto-config policy.	string	Maximum length: 63	default

config switch-controller initial-config template

Configure template for auto-generated VLANs.

```

config switch-controller initial-config template
    Description: Configure template for auto-generated VLANs.
    edit <name>
        set vlanid {integer}

```

```

set ip {ipv4-classnet-host}
set allowaccess {option1}, {option2}, ...
set auto-ip [enable|disable]
set dhcp-server [enable|disable]
next
end

```

config switch-controller initial-config template

Parameter	Description	Type	Size	Default
vlanid	Unique VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0
ip	Interface IPv4 address and subnet mask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
allowaccess	Permitted types of management access to this interface.	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.		
auto-ip	Automatically allocate interface address and subnet block.	option	-	enable
Option		Description		
		<i>enable</i> Enable auto-ip status.		
		<i>disable</i> Disable auto-ip status.		

Parameter	Description	Type	Size	Default
dhcp-server	Enable/disable a DHCP server on this interface.	option	-	disable
Option	Description			
<i>enable</i>	Enable DHCP server.			
<i>disable</i>	Disable DHCP server.			

config switch-controller initial-config vlans

Configure initial template for auto-generated VLAN interfaces.

```
config switch-controller initial-config vlans
    Description: Configure initial template for auto-generated VLAN interfaces.
    set default-vlan {string}
    set quarantine {string}
    set rspan {string}
    set voice {string}
    set video {string}
    set nac {string}
    set nac-segment {string}
end
```

config switch-controller initial-config vlans

Parameter	Description	Type	Size	Default
default-vlan	Default VLAN (native) assigned to all switch ports upon discovery.	string	Maximum length: 63	_default
quarantine	VLAN for quarantined traffic.	string	Maximum length: 63	quarantine
rspan	VLAN for RSPAN/ERSPAN mirrored traffic.	string	Maximum length: 63	rspan
voice	VLAN dedicated for voice devices.	string	Maximum length: 63	voice
video	VLAN dedicated for video devices.	string	Maximum length: 63	video
nac	VLAN for NAC onboarding devices.	string	Maximum length: 63	onboarding
nac-segment	VLAN for NAC segment primary interface.	string	Maximum length: 63	nac_segment

config switch-controller switch-profile

Configure FortiSwitch switch profile.

```
config switch-controller switch-profile
    Description: Configure FortiSwitch switch profile.
    edit <name>
        set login-passwd-override [enable|disable]
        set login-passwd {password}
    next
end
```

config switch-controller switch-profile

Parameter	Description	Type	Size	Default
login-passwd-override	Enable/disable overriding the admin administrator password for a managed FortiSwitch with the FortiGate admin administrator account password.	option	-	disable
Option		Description		
		enable	Override a managed FortiSwitch's admin administrator password.	
		disable	Use the managed FortiSwitch admin administrator account password.	
login-passwd	Login password of managed FortiSwitch.	password	Not Specified	

config switch-controller custom-command

Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices.

```
config switch-controller custom-command
    Description: Configure the FortiGate switch controller to send custom commands to managed
                 FortiSwitch devices.
    edit <command-name>
        set description {string}
        set command {var-string}
    next
end
```

config switch-controller custom-command

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
command	String of commands to send to FortiSwitch devices (For example (%0a = return key): config switch trunk %0a edit myTrunk %0a set members port1 port2 %0a end %0a).	var-string	Maximum length: 4095	

config switch-controller virtual-port-pool

Configure virtual pool.

```
config switch-controller virtual-port-pool
    Description: Configure virtual pool.
    edit <name>
        set description {string}
    next
end
```

config switch-controller virtual-port-pool

Parameter	Description	Type	Size	Default
description	Virtual switch pool description.	string	Maximum length: 63	

config switch-controller ptp settings

Global PTP settings.

```
config switch-controller ptp settings
    Description: Global PTP settings.
    set mode [disable|transparent-e2e|...]
end
```

config switch-controller ptp settings

Parameter	Description	Type	Size	Default
mode	Enable/disable PTP mode.	option	-	disable
Option	Description			
<i>disable</i>	Disable PTP function. Packets are forwarded with no action.			
<i>transparent-e2e</i>	Enable end-to-end transparent clock.			
<i>transparent-p2p</i>	Enable peer-to-peer transparent clock.			

config switch-controller ptpt policy

PTP policy configuration.

```
config switch-controller ptpt policy
    Description: PTP policy configuration.
    edit <name>
        set status [disable|enable]
    next
end
```

config switch-controller ptpt policy

Parameter	Description	Type	Size	Default
status	Enable/disable PTP policy.	option	-	enable
Parameter	Description	Type	Size	Default
Option	Description			
disable	Disable PTP policy.			
enable	Enable PTP policy.			

config switch-controller vlan-policy

Configure VLAN policy to be applied on the managed FortiSwitch ports through dynamic-port-policy.

```
config switch-controller vlan-policy
    Description: Configure VLAN policy to be applied on the managed FortiSwitch ports through
                dynamic-port-policy.
    edit <name>
        set description {string}
        set fortalink {string}
        set vlan {string}
        set allowed-vlans <vlan-name1>, <vlan-name2>, ...
        set untagged-vlans <vlan-name1>, <vlan-name2>, ...
        set allowed-vlans-all [enable|disable]
        set discard-mode [none|all-untagged|...]
    next
end
```

config switch-controller vlan-policy

Parameter	Description	Type	Size	Default
description	Description for the VLAN policy.	string	Maximum length: 63	
fortalink	FortiLink interface for which this VLAN policy belongs to.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
vlan	Native VLAN to be applied when using this VLAN policy.	string	Maximum length: 15	
allowed-vlans <vlan-name>	Allowed VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79	
untagged-vlans <vlan-name>	Untagged VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79	
allowed-vlans-all	Enable/disable all defined VLANs when using this VLAN policy.	option	-	disable
Option	Description			
<i>enable</i>	Enable all defined VLANs.			
<i>disable</i>	Disable all defined VLANs.			
discard-mode	Discard mode to be applied when using this VLAN policy.	option	-	none
Option	Description			
<i>none</i>	Discard disabled.			
<i>all-untagged</i>	Discard all frames that are untagged.			
<i>all-tagged</i>	Discard all frames that are tagged.			

config switch-controller dynamic-port-policy

Configure Dynamic port policy to be applied on the managed FortiSwitch ports through DPP device.

```
config switch-controller dynamic-port-policy
  Description: Configure Dynamic port policy to be applied on the managed FortiSwitch ports
    through DPP device.
  edit <name>
    set description {string}
    set fortilink {string}
    config policy
      Description: Port policies with matching criteria and actions.
      edit <name>
        set description {string}
        set status [enable|disable]
        set category [device|interface-tag]
        set interface-tags <tag-name1>, <tag-name2>, ...
        set mac {string}
        set type {string}
        set family {string}
        set host {string}
```

```

        set lldp-profile {string}
        set qos-policy {string}
        set 802-1x {string}
        set vlan-policy {string}
        set bounce-port-link [disable|enable]
    next
end
next
end

```

config switch-controller dynamic-port-policy

Parameter	Description	Type	Size	Default
description	Description for the Dynamic port policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this Dynamic port policy belongs to.	string	Maximum length: 15	

config policy

Parameter	Description	Type	Size	Default
description	Description for the policy.	string	Maximum length: 63	
status	Enable/disable policy.	option	-	enable
Option		Description		
		enable Enable policy.		
		disable Disable policy.		
category	Category of Dynamic port policy.	option	-	device
Option		Description		
		device Device category.		
		interface-tag Interface Tag category.		
interface-tags <tag-name>	Policy matching the FortiSwitch interface object tags. FortiSwitch port tag name.	string	Maximum length: 63	
mac	Policy matching MAC address.	string	Maximum length: 17	
type	Policy matching type.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
family	Policy matching family.	string	Maximum length: 31	
host	Policy matching host.	string	Maximum length: 64	
lldp-profile	LLDP profile to be applied when using this policy.	string	Maximum length: 63	
qos-policy	QoS policy to be applied when using this policy.	string	Maximum length: 63	
802-1x	802.1x security policy to be applied when using this policy.	string	Maximum length: 31	
vlan-policy	VLAN policy to be applied when using this policy.	string	Maximum length: 63	
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied. Helps to clear and reassign VLAN from lldp-profile.	option	-	enable
Option	Description			
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.			
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.			

config switch-controller managed-switch

Configure FortiSwitch devices that are managed by this FortiGate.

```
config switch-controller managed-switch
  Description: Configure FortiSwitch devices that are managed by this FortiGate.
  edit <switch-id>
    set name {string}
    set description {string}
    set switch-profile {string}
    set access-profile {string}
    set fsw-wan1-peer {string}
    set fsw-wan1-admin [discovered|disable|...]
    set poe-pre-standard-detection [enable|disable]
    set dhcp-server-access-list [global|enable|...]
    set poe-detection-type {integer}
    set directly-connected {integer}
    set version {integer}
    set max-allowed-trunk-members {integer}
    set pre-provisioned {integer}
    set l3-discovered {integer}
    set tdr-supported {string}
    set dynamic-capability {user}
    set switch-device-tag {string}
```

```
set switch-dhcp_opt43_key {string}
set mclag-igmp-snooping-aware [enable|disable]
set dynamically-discovered {integer}
set type [virtual|physical]
set owner-vdom {string}
set flow-identity {user}
set staged-image-version {string}
set delayed-restart-trigger {integer}
set firmware-provision [enable|disable]
set firmware-provision-version {string}
config ports
    Description: Managed-switch port list.
    edit <port-name>
        set port-owner {string}
        set switch-id {string}
        set speed [10half|10full|...]
        set status [up|down]
        set poe-status [enable|disable]
        set ip-source-guard [disable|enable]
        set ptp-policy {string}
        set aggregator-mode [bandwidth|count]
        set rpvst-port [disabled|enabled]
        set poe-pre-standard-detection [enable|disable]
        set port-number {integer}
        set port-prefix-type {integer}
        set fortalink-port {integer}
        set poe-capable {integer}
        set stacking-port {integer}
        set p2p-port {integer}
        set mclag-ic平-port {integer}
        set fiber-port {integer}
        set media-type {string}
        set poe-standard {string}
        set poe-max-power {string}
        set flags {integer}
        set isl-local-trunk-name {string}
        set isl-peer-port-name {string}
        set isl-peer-device-name {string}
        set fgt-peer-port-name {string}
        set fgt-peer-device-name {string}
        set vlan {string}
        set allowed-vlans-all [enable|disable]
        set allowed-vlans <vlan-name1>, <vlan-name2>, ...
        set untagged-vlans <vlan-name1>, <vlan-name2>, ...
        set type [physical|trunk]
        set access-mode [dynamic|nac|...]
        set matched-dpp-policy {string}
        set matched-dpp-intf-tags {string}
        set dhcp-snooping [untrusted|trusted]
        set dhcp-snoop-option82-trust [enable|disable]
        set arp-inspection-trust [untrusted|trusted]
        set igmps-flood-reports [enable|disable]
        set igmps-flood-traffic [enable|disable]
        set stp-state [enabled|disabled]
        set stp-root-guard [enabled|disabled]
        set stp-bpdu-guard [enabled|disabled]
        set stp-bpdu-guard-timeout {integer}
```

```

        set edge-port [enable|disable]
        set discard-mode [none|all-untagged|...]
        set packet-sampler [enabled|disabled]
        set packet-sample-rate {integer}
        set sflow-counter-interval {integer}
        set sample-direction [tx|rx|...]
        set fec-capable {integer}
        set fec-state [disabled|cl74|...]
        set flow-control [disable|tx|...]
        set pause-meter {integer}
        set pause-meter-resume [75%|50%|...]
        set loop-guard [enabled|disabled]
        set loop-guard-timeout {integer}
        set port-policy {string}
        set qos-policy {string}
        set storm-control-policy {string}
        set port-security-policy {string}
        set export-to-pool {string}
        set export-tags <tag-name1>, <tag-name2>, ...
        set learning-limit {integer}
        set sticky-mac [enable|disable]
        set lldp-status [disable|rx-only|...]
        set lldp-profile {string}
        set export-to {string}
        set mac-addr {mac-address}
        set port-selection-criteria [src-mac|dst-mac|...]
        set description {string}
        set lacp-speed [slow|fast]
        set mode [static|lacp-passive|...]
        set bundle [enable|disable]
        set member-withdrawal-behavior [forward|block]
        set mclag [enable|disable]
        set min-bundle {integer}
        set max-bundle {integer}
        set members <member-name1>, <member-name2>, ...
    next
end
config ip-source-guard
    Description: IP source guard.
    edit <port>
        set description {string}
        config binding-entry
            Description: IP and MAC address configuration.
            edit <entry-name>
                set ip {ipv4-address-any}
                set mac {mac-address}
            next
        end
    next
end
config stp-settings
    Description: Configuration method to edit Spanning Tree Protocol (STP) settings used
        to prevent bridge loops.
    set local-override [enable|disable]
    set name {string}
    set revision {integer}
    set hello-time {integer}

```

```

        set forward-time {integer}
        set max-age {integer}
        set max-hops {integer}
        set pending-timer {integer}
    end
    config stp-instance
        Description: Configuration method to edit Spanning Tree Protocol (STP) instances.
        edit <id>
            set priority [0|4096|...]
        next
    end
    set override-snmp-sysinfo [disable|enable]
    config snmp-sysinfo
        Description: Configuration method to edit Simple Network Management Protocol (SNMP)
                    system info.
        set status [disable|enable]
        set engine-id {string}
        set description {string}
        set contact-info {string}
        set location {string}
    end
    set override-snmp-trap-threshold [enable|disable]
    config snmp-trap-threshold
        Description: Configuration method to edit Simple Network Management Protocol (SNMP)
                    trap threshold values.
        set trap-high-cpu-threshold {integer}
        set trap-low-memory-threshold {integer}
        set trap-log-full-threshold {integer}
    end
    set override-snmp-community [enable|disable]
    config snmp-community
        Description: Configuration method to edit Simple Network Management Protocol (SNMP)
                    communities.
        edit <id>
            set name {string}
            set status [disable|enable]
            config hosts
                Description: Configure IPv4 SNMP managers (hosts).
                edit <id>
                    set ip {user}
                next
            end
            set query-v1-status [disable|enable]
            set query-v1-port {integer}
            set query-v2c-status [disable|enable]
            set query-v2c-port {integer}
            set trap-v1-status [disable|enable]
            set trap-v1-lport {integer}
            set trap-v1-rport {integer}
            set trap-v2c-status [disable|enable]
            set trap-v2c-lport {integer}
            set trap-v2c-rport {integer}
            set events {option1}, {option2}, ...
        next
    end
    set override-snmp-user [enable|disable]
    config snmp-user

```

```

Description: Configuration method to edit Simple Network Management Protocol (SNMP)
    users.
edit <name>
    set queries [disable|enable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
    set auth-proto [md5|sha1|...]
    set auth-pwd {password}
    set priv-proto [aes128|aes192|...]
    set priv-pwd {password}
next
end
set qos-drop-policy [taildrop|random-early-detection]
set qos-red-probability {integer}
config switch-log
    Description: Configuration method to edit FortiSwitch logging settings (logs are
        transferred to and inserted into the FortiGate event log).
    set local-override [enable|disable]
    set status [enable|disable]
    set severity [emergency|alert|...]
end
config remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
edit <name>
    set status [enable|disable]
    set server {string}
    set port {integer}
    set severity [emergency|alert|...]
    set csv [enable|disable]
    set facility [kernel|user|...]
next
end
config storm-control
    Description: Configuration method to edit FortiSwitch storm control for measuring
        traffic activity using data rates to prevent traffic disruption.
    set local-override [enable|disable]
    set rate {integer}
    set unknown-unicast [enable|disable]
    set unknown-multicast [enable|disable]
    set broadcast [enable|disable]
end
config mirror
    Description: Configuration method to edit FortiSwitch packet mirror.
edit <name>
    set status [active|inactive]
    set switching-packet [enable|disable]
    set dst {string}
    set src-ingress <name1>, <name2>, ...
    set src-egress <name1>, <name2>, ...
next
end
config static-mac
    Description: Configuration method to edit FortiSwitch Static and Sticky MAC.
edit <id>
    set type [static|sticky]
    set vlan {string}
    set mac {mac-address}

```

```

        set interface {string}
        set description {string}
    next
end
config custom-command
    Description: Configuration method to edit FortiSwitch commands to be pushed to this
        FortiSwitch device upon rebooting the FortiGate switch controller or the
        FortiSwitch.
    edit <command-entry>
        set command-name {string}
    next
end
config igmp-snooping
    Description: Configure FortiSwitch IGMP snooping global settings.
    set local-override [enable|disable]
    set aging-time {integer}
    set flood-unknown-multicast [enable|disable]
end
config 802-1X-settings
    Description: Configuration method to edit FortiSwitch 802.1X global settings.
    set local-override [enable|disable]
    set link-down-auth [set-unauth|no-action]
    set reauth-period {integer}
    set max-reauth-attempt {integer}
    set tx-period {integer}
end
next
end

```

config switch-controller managed-switch

Parameter	Description	Type	Size	Default
name	Managed-switch name.	string	Maximum length: 35	
description	Description.	string	Maximum length: 63	
switch-profile	FortiSwitch profile.	string	Maximum length: 35	default
access-profile	FortiSwitch access profile.	string	Maximum length: 31	default
fsw-wan1-peer	Fortiswitch WAN1 peer port.	string	Maximum length: 35	
fsw-wan1-admin	FortiSwitch WAN1 admin status; enable to authorize the FortiSwitch as a managed switch.	option	-	discovered

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discovered</i>	Link waiting to be authorized.		
	<i>disable</i>	Link unauthorized.		
	<i>enable</i>	Link authorized.		
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PoE pre-standard detection.		
	<i>disable</i>	Disable PoE pre-standard detection.		
dhcp-server-access-list	DHCP snooping server access list.	option	-	global
	Option	Description		
	<i>global</i>	Use global setting for DHCP snooping server access list.		
	<i>enable</i>	Override global setting and enable DHCP server access list.		
	<i>disable</i>	Override global setting and disable DHCP server access list.		
poe-detection-type	PoE detection type for FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0
directly-connected	Directly connected FortiSwitch.	integer	Minimum value: 0 Maximum value: 1	0
version	FortiSwitch version.	integer	Minimum value: 0 Maximum value: 255	0
max-allowed-trunk-members	FortiSwitch maximum allowed trunk members.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default						
owner-vdom	VDOM which owner of port belongs to.	string	Maximum length: 31							
flow-identity	Flow-tracking netflow ipfix switch identity in hex format.	user	Not Specified	00000000						
staged-image-version	Staged image version for FortiSwitch.	string	Maximum length: 127							
delayed-restart-trigger	Delayed restart triggered for this FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0						
firmware-provision	Enable/disable provisioning of firmware to FortiSwitches on join connection.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><code>enable</code></td><td>Enable firmware-provision.</td></tr> <tr> <td><code>disable</code></td><td>Disable firmware-provision.</td></tr> </tbody> </table>					Option	Description	<code>enable</code>	Enable firmware-provision.	<code>disable</code>	Disable firmware-provision.
Option	Description									
<code>enable</code>	Enable firmware-provision.									
<code>disable</code>	Disable firmware-provision.									
firmware-provision-version	Firmware version to provision to this FortiSwitch on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35							
override-snmp-sysinfo	Enable/disable overriding the global SNMP system information.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><code>disable</code></td><td>Use the global SNMP system information.</td></tr> <tr> <td><code>enable</code></td><td>Override the global SNMP system information.</td></tr> </tbody> </table>					Option	Description	<code>disable</code>	Use the global SNMP system information.	<code>enable</code>	Override the global SNMP system information.
Option	Description									
<code>disable</code>	Use the global SNMP system information.									
<code>enable</code>	Override the global SNMP system information.									
override-snmp-trap-threshold	Enable/disable overriding the global SNMP trap threshold values.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><code>enable</code></td><td>Override the global SNMP trap threshold values.</td></tr> </tbody> </table>					Option	Description	<code>enable</code>	Override the global SNMP trap threshold values.		
Option	Description									
<code>enable</code>	Override the global SNMP trap threshold values.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Use the global SNMP trap threshold values.		
override-snmp-community	Enable/disable overriding the global SNMP communities.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the global SNMP communities.		
	<i>disable</i>	Use the global SNMP communities.		
override-snmp-user	Enable/disable overriding the global SNMP users.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the global SNMPv3 users.		
	<i>disable</i>	Use the global SNMPv3 users.		
qos-drop-policy	Set QoS drop-policy.	option	-	taildrop
	Option	Description		
	<i>taildrop</i>	Taildrop policy.		
	<i>random-early-detection</i>	Random early detection drop policy.		
qos-red-probability	Set QoS RED/WRED drop probability.	integer	Minimum value: 0 Maximum value: 100	12

config ports

Parameter	Description	Type	Size	Default
port-owner	Switch port name.	string	Maximum length: 15	
switch-id	Switch id.	string	Maximum length: 16	
speed	Switch port speed; default and available settings depend on hardware.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>10half</i>	10M half-duplex.		
	<i>10full</i>	10M full-duplex.		
	<i>100half</i>	100M half-duplex.		
	<i>100full</i>	100M full-duplex.		
	<i>1000auto</i>	Auto-negotiation (1G full-duplex only).		
	<i>1000fiber</i>	1G full-duplex (fiber SFPs only)		
	<i>1000full</i>	1G full-duplex		
	<i>10000</i>	10G full-duplex		
	<i>40000</i>	40G full-duplex		
	<i>auto</i>	Auto-negotiation.		
	<i>auto-module</i>	Auto Module.		
	<i>100FX-half</i>	100Mbps half-duplex. 100Base-FX.		
	<i>100FX-full</i>	100Mbps full-duplex. 100Base-FX.		
	<i>100000full</i>	100Gbps full-duplex.		
	<i>2500auto</i>	Auto-Negotiation (2.5Gbps Only).		
	<i>25000full</i>	25Gbps full-duplex.		
	<i>50000full</i>	50Gbps full-duplex.		
	<i>10000cr</i>	10Gbps copper interface.		
	<i>10000sr</i>	10Gbps SFI interface.		
	<i>100000sr4</i>	100Gbps SFI interface.		
	<i>100000cr4</i>	100Gbps copper interface.		
	<i>25000cr4</i>	25Gbps copper interface.		
	<i>25000sr4</i>	25Gbps SFI interface.		
	<i>5000full</i>	5Gbps full-duplex.		
status	Switch port admin status: up or down.	option	-	up
	Option	Description		
	<i>up</i>	Set admin status up.		
	<i>down</i>	Set admin status down.		

Parameter	Description	Type	Size	Default
poe-status	Enable/disable PoE status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable PoE status.		
	<i>disable</i>	Disable PoE status.		
ip-source-guard	Enable/disable IP source guard.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable IP source guard.		
	<i>enable</i>	Enable IP source guard.		
ptp-policy	PTP policy configuration.	string	Maximum length: 63	default
aggregator-mode	LACP member select mode.	option	-	bandwidth
	Option	Description		
	<i>bandwidth</i>	Member selection based on largest total bandwidth of links of similar speed.		
	<i>count</i>	Member selection based on largest count of similar link speed.		
rpvst-port	Enable/disable inter-operability with rapid PVST on this interface.	option	-	disabled
	Option	Description		
	<i>disabled</i>	Disable inter-operability with rapid PVST on this interface.		
	<i>enabled</i>	Enable inter-operability with rapid PVST on this interface.		
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PoE pre-standard detection.		
	<i>disable</i>	Disable PoE pre-standard detection.		
port-number	Port number.	integer	Minimum value: 1 Maximum value: 64	0

Parameter	Description	Type	Size	Default
port-prefix-type	Port prefix type.	integer	Minimum value: 0 Maximum value: 1	0
fortilink-port	FortiLink uplink port.	integer	Minimum value: 0 Maximum value: 1	0
poe-capable	PoE capable.	integer	Minimum value: 0 Maximum value: 1	0
stacking-port	Stacking port.	integer	Minimum value: 0 Maximum value: 1	0
p2p-port	General peer to peer tunnel port.	integer	Minimum value: 0 Maximum value: 1	0
mclag-icl-port	MCLAG-ICL port.	integer	Minimum value: 0 Maximum value: 1	0
fiber-port	Fiber-port.	integer	Minimum value: 0 Maximum value: 1	0
media-type	Media type.	string	Maximum length: 31	
poe-standard	PoE standard supported.	string	Maximum length: 63	
poe-max-power	PoE maximum power.	string	Maximum length: 35	
flags	Port properties flags.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
isl-local-trunk-name	ISL local trunk name.	string	Maximum length: 15									
isl-peer-port-name	ISL peer port name.	string	Maximum length: 15									
isl-peer-device-name	ISL peer device name.	string	Maximum length: 16									
fgt-peer-port-name	FGT peer port name.	string	Maximum length: 15									
fgt-peer-device-name	FGT peer device name.	string	Maximum length: 16									
vlan	Assign switch ports to a VLAN.	string	Maximum length: 15									
allowed-vlans-all	Enable/disable all defined vlans on this port.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable all defined VLANs on this port.</td></tr> <tr> <td><i>disable</i></td><td>Disable all defined VLANs on this port.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable all defined VLANs on this port.	<i>disable</i>	Disable all defined VLANs on this port.		
Option	Description											
<i>enable</i>	Enable all defined VLANs on this port.											
<i>disable</i>	Disable all defined VLANs on this port.											
allowed-vlans <vlan-name>	Configure switch port tagged vlans VLAN name.	string	Maximum length: 79									
untagged-vlans <vlan-name>	Configure switch port untagged vlans VLAN name.	string	Maximum length: 79									
type	Interface type: physical or trunk port.	option	-	physical								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>physical</i></td><td>Physical port.</td></tr> <tr> <td><i>trunk</i></td><td>Trunk port.</td></tr> </tbody> </table>					Option	Description	<i>physical</i>	Physical port.	<i>trunk</i>	Trunk port.		
Option	Description											
<i>physical</i>	Physical port.											
<i>trunk</i>	Trunk port.											
access-mode	Access mode of the port.	option	-	static								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>dynamic</i></td><td>Dynamic mode.</td></tr> <tr> <td><i>nac</i></td><td>NAC mode.</td></tr> <tr> <td><i>static</i></td><td>Static mode.</td></tr> </tbody> </table>					Option	Description	<i>dynamic</i>	Dynamic mode.	<i>nac</i>	NAC mode.	<i>static</i>	Static mode.
Option	Description											
<i>dynamic</i>	Dynamic mode.											
<i>nac</i>	NAC mode.											
<i>static</i>	Static mode.											

Parameter	Description	Type	Size	Default
matched-dpp-policy	Matched child policy in the dynamic port policy.	string	Maximum length: 63	
matched-dpp-intf-tags	Matched interface tags in the dynamic port policy.	string	Maximum length: 63	
dhcp-snooping	Trusted or untrusted DHCP-snooping interface.	option	-	untrusted
	Option	Description		
	<i>untrusted</i>	Untrusted DHCP snooping interface.		
	<i>trusted</i>	Trusted DHCP snooping interface.		
dhcp-snoop-option82-trust	Enable/disable allowance of DHCP with option-82 on untrusted interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.		
	<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.		
arp-inspection-trust	Trusted or untrusted dynamic ARP inspection.	option	-	untrusted
	Option	Description		
	<i>untrusted</i>	Untrusted dynamic ARP inspection.		
	<i>trusted</i>	Trusted dynamic ARP inspection.		
igmps-flood-reports	Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.		
	<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.		
igmps-flood-traffic	Enable/disable flooding of IGMP snooping traffic to this interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.		
	<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.		

Parameter	Description	Type	Size	Default
stp-state	Enable/disable Spanning Tree Protocol (STP) on this interface.	option	-	enabled
	Option	Description		
	<i>enabled</i>	Enable STP on this interface.		
	<i>disabled</i>	Disable STP on this interface.		
stp-root-guard	Enable/disable STP root guard on this interface.	option	-	disabled
	Option	Description		
	<i>enabled</i>	Enable STP root-guard on this interface.		
	<i>disabled</i>	Disable STP root-guard on this interface.		
stp-bpdu-guard	Enable/disable STP BPDU guard on this interface.	option	-	disabled
	Option	Description		
	<i>enabled</i>	Enable STP BPDU guard on this interface.		
	<i>disabled</i>	Disable STP BPDU guard on this interface.		
stp-bpdu-guard-timeout	BPDU Guard disabling protection .	integer	Minimum value: 0 Maximum value: 120	5
edge-port	Enable/disable this interface as an edge port, bridging connections between workstations and/or computers.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this interface as an edge port.		
	<i>disable</i>	Disable this interface as an edge port.		
discard-mode	Configure discard mode for port.	option	-	none
	Option	Description		
	<i>none</i>	Discard disabled.		
	<i>all-untagged</i>	Discard all frames that are untagged.		
	<i>all-tagged</i>	Discard all frames that are tagged.		

Parameter	Description	Type	Size	Default
packet-sampler	Enable/disable packet sampling on this interface.	option	-	disabled
	Option	Description		
	<i>enabled</i>	Enable packet sampling on this interface.		
	<i>disabled</i>	Disable packet sampling on this interface.		
packet-sample-rate	Packet sampling rate .	integer	Minimum value: 0 Maximum value: 99999	512
sflow-counter-interval	sFlow sampling counter polling interval .	integer	Minimum value: 0 Maximum value: 255	0
sample-direction	Packet sampling direction.	option	-	both
	Option	Description		
	<i>tx</i>	Monitor transmitted traffic.		
	<i>rx</i>	Monitor received traffic.		
	<i>both</i>	Monitor transmitted and received traffic.		
fec-capable	FEC capable.	integer	Minimum value: 0 Maximum value: 1	0
fec-state	State of forward error correction.	option	-	cl91
	Option	Description		
	<i>disabled</i>	Disable forward error correction.		
	<i>cl74</i>	Enable Clause 74 FC-FEC, which only applies to 25Gbps.		
	<i>cl91</i>	Enable Clause 91 RS-FEC, which only applies to 100Gbps.		
flow-control	Flow control direction.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable flow control.		
	<i>tx</i>	Enable flow control for transmission pause control frames.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>rx</i>	Enable flow control for receive pause control frames.		
	<i>both</i>	Enable flow control for both transmission and receive pause control frames.		
pause-meter	Configure ingress pause metering rate, in kbps .	integer	Minimum value: 128 Maximum value: 2147483647	0
pause-meter-resume	Resume threshold for resuming traffic on ingress port.	option	-	50%
	Option	Description		
	75%	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.		
	50%	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.		
	25%	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.		
loop-guard	Enable/disable loop-guard on this interface, an STP optimization used to prevent network loops.	option	-	disabled
	Option	Description		
	<i>enabled</i>	Enable loop-guard on this interface.		
	<i>disabled</i>	Disable loop-guard on this interface.		
loop-guard-timeout	Loop-guard timeout .	integer	Minimum value: 0 Maximum value: 120	45
port-policy	Switch controller dynamic port policy from available options.	string	Maximum length: 63	
qos-policy	Switch controller QoS policy from available options.	string	Maximum length: 63	default
storm-control-policy	Switch controller storm control policy from available options.	string	Maximum length: 63	default

Parameter	Description	Type	Size	Default										
port-security-policy	Switch controller authentication policy to apply to this managed switch from available options.	string	Maximum length: 31											
export-to-pool	Switch controller export port to pool-list.	string	Maximum length: 35											
export-tags <tag-name>	Configure export tag(s) for FortiSwitch port when exported to a virtual port pool. FortiSwitch port tag name when exported to a virtual port pool.	string	Maximum length: 63											
learning-limit	Limit the number of dynamic MAC addresses on this Port .	integer	Minimum value: 0 Maximum value: 128	0										
sticky-mac	Enable or disable sticky-mac on the interface.	option	-	disable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable sticky mac on the interface.</td></tr> <tr> <td>disable</td><td>Disable sticky mac on the interface.</td></tr> </tbody> </table>					Option	Description	enable	Enable sticky mac on the interface.	disable	Disable sticky mac on the interface.				
Option	Description													
enable	Enable sticky mac on the interface.													
disable	Disable sticky mac on the interface.													
lldp-status	LLDP transmit and receive status.	option	-	tx-rx										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>disable</td><td>Disable LLDP TX and RX.</td></tr> <tr> <td>rx-only</td><td>Enable LLDP as RX only.</td></tr> <tr> <td>tx-only</td><td>Enable LLDP as TX only.</td></tr> <tr> <td>tx-rx</td><td>Enable LLDP TX and RX.</td></tr> </tbody> </table>					Option	Description	disable	Disable LLDP TX and RX.	rx-only	Enable LLDP as RX only.	tx-only	Enable LLDP as TX only.	tx-rx	Enable LLDP TX and RX.
Option	Description													
disable	Disable LLDP TX and RX.													
rx-only	Enable LLDP as RX only.													
tx-only	Enable LLDP as TX only.													
tx-rx	Enable LLDP TX and RX.													
lldp-profile	LLDP port TLV profile.	string	Maximum length: 63	default-auto-isl										
export-to	Export managed-switch port to a tenant VDOM.	string	Maximum length: 31											
mac-addr	Port/Trunk MAC.	mac-address	Not Specified	00:00:00:00:00:00										
port-selection-criteria	Algorithm for aggregate port selection.	option	-	src-dst-ip										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>src-mac</i>	Source MAC address.		
	<i>dst-mac</i>	Destination MAC address.		
	<i>src-dst-mac</i>	Source and destination MAC address.		
	<i>src-ip</i>	Source IP address.		
	<i>dst-ip</i>	Destination IP address.		
	<i>src-dst-ip</i>	Source and destination IP address.		
description	Description for port.	string	Maximum length: 63	
lacp-speed	Send Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second (fast).	option	-	slow
	Option	Description		
	<i>slow</i>	Send LACP message every 30 seconds.		
	<i>fast</i>	Send LACP message every second.		
mode	LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.	option	-	static
	Option	Description		
	<i>static</i>	Static aggregation, do not send and ignore any control messages.		
	<i>lacp-passive</i>	Passively use LACP to negotiate 802.3ad aggregation.		
	<i>lacp-active</i>	Actively use LACP to negotiate 802.3ad aggregation.		
bundle	Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable bundling.		
	<i>disable</i>	Disable bundling.		
member-withdrawal-behavior	Port behavior after it withdraws because of loss of control packets.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>forward</i>	Forward traffic.		
	<i>block</i>	Block traffic.		
mclag	Enable/disable multi-chassis link aggregation (MCLAG).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable MCLAG.		
	<i>disable</i>	Disable MCLAG.		
min-bundle	Minimum size of LAG bundle	integer	Minimum value: 1 Maximum value: 24	1
max-bundle	Maximum size of LAG bundle	integer	Minimum value: 1 Maximum value: 24	24
members <member-name>	Aggregated LAG bundle interfaces. Interface name from available options.	string	Maximum length: 79	

config ip-source-guard

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	

config binding-entry

Parameter	Description	Type	Size	Default
ip	Source IP for this rule.	ipv4-address-any	Not Specified	0.0.0.0
mac	MAC address for this rule.	mac-address	Not Specified	00:00:00:00:00:00

config stp-settings

Parameter	Description	Type	Size	Default
local-override	Enable to configure local STP settings that override global STP settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override global STP settings.		
	<i>disable</i>	Use global STP settings.		
name	Name of local STP settings configuration.	string	Maximum length: 31	
revision	STP revision number .	integer	Minimum value: 0 Maximum value: 65535	0
hello-time	Period of time between successive STP frame Bridge Protocol Data Units .	integer	Minimum value: 1 Maximum value: 10	2
forward-time	Period of time a port is in listening and learning state .	integer	Minimum value: 4 Maximum value: 30	15
max-age	Maximum time before a bridge port saves its configuration BPDU information .	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops between the root bridge and the furthest bridge .	integer	Minimum value: 1 Maximum value: 40	20
pending-timer	Pending time .	integer	Minimum value: 1 Maximum value: 15	4

config stp-instance

Parameter	Description	Type	Size	Default
priority	Priority.	option	-	32768

Parameter	Description	Type	Size	Default
	Option	Description		
	0	0.		
	4096	4096.		
	8192	8192.		
	12288	12288.		
	16384	16384.		
	20480	20480.		
	24576	24576.		
	28672	28672.		
	32768	32768.		
	36864	36864.		
	40960	40960.		
	45056	45056.		
	49152	49152.		
	53248	53248.		
	57344	57344.		
	61440	61440.		

config snmp-sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable
	Option	Description		
	disable	Disable SNMP.		
	enable	Enable SNMP.		
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24	
description	System description.	string	Maximum length: 35	
contact-info	Contact information.	string	Maximum length: 35	
location	System location.	string	Maximum length: 35	

config snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90

config snmp-community

Parameter	Description	Type	Size	Default
name	SNMP community name.	string	Maximum length: 35	
status	Enable/disable this SNMP community.	option	-	enable
Option		Description		
		<i>disable</i> Disable SNMP community.		
		<i>enable</i> Enable SNMP community.		
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable
Option		Description		
		<i>disable</i> Disable SNMP v1 queries.		
		<i>enable</i> Enable SNMP v1 queries.		
query-v1-port	SNMP v1 query port .	integer	Minimum value: 0 Maximum value: 65535	161

Parameter	Description	Type	Size	Default
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c queries.		
	<i>enable</i>	Enable SNMP v2c queries.		
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535	161
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v1 traps.		
	<i>enable</i>	Enable SNMP v1 traps.		
trap-v1-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c traps.		
	<i>enable</i>	Enable SNMP v2c traps.		
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip ent-conf-change
Option	Description			
<i>cpu-high</i>	Send a trap when CPU usage too high.			
<i>mem-low</i>	Send a trap when available memory is low.			
<i>log-full</i>	Send a trap when log disk space becomes low.			
<i>intf-ip</i>	Send a trap when an interface IP address is changed.			
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).			

config hosts

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

config snmp-user

Parameter	Description	Type	Size	Default
queries	Enable/disable SNMP queries for this user.	option	-	enable
Option	Description			
<i>disable</i>	Disable SNMP queries for this user.			
<i>enable</i>	Enable SNMP queries for this user.			
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).		
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).		
	<i>auth-priv</i>	Message with authentication and privacy (encryption).		
auth-proto	Authentication protocol.	option	-	sha256
	Option	Description		
	<i>md5</i>	HMAC-MD5-96 authentication protocol.		
	<i>sha1</i>	HMAC-SHA-1 authentication protocol.		
	<i>sha224</i>	HMAC-SHA-224 authentication protocol.		
	<i>sha256</i>	HMAC-SHA-256 authentication protocol.		
	<i>sha384</i>	HMAC-SHA-384 authentication protocol.		
	<i>sha512</i>	HMAC-SHA-512 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes128
	Option	Description		
	<i>aes128</i>	CFB128-AES-128 symmetric encryption protocol.		
	<i>aes192</i>	CFB128-AES-192 symmetric encryption protocol.		
	<i>aes192c</i>	CFB128-AES-192-C symmetric encryption protocol.		
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.		
	<i>aes256c</i>	CFB128-AES-256-C symmetric encryption protocol.		
	<i>des</i>	CBC-DES symmetric encryption protocol.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

config switch-log

Parameter	Description	Type	Size	Default
local-override	Enable to configure local logging settings that override global logging settings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Override global logging settings.		
	<i>disable</i>	Use global logging settings.		
status	Enable/disable adding FortiSwitch logs to the FortiGate event log.	option	-	enable
	Option	Description		
	<i>enable</i>	Add FortiSwitch logs to the FortiGate event log.		
	<i>disable</i>	Do not add FortiSwitch logs to the FortiGate event log.		
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		

config remote-log

Parameter	Description	Type	Size	Default
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disabled
	Option	Description		
	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.		
	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.		
server	IPv4 address of the remote syslog server.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default																				
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514																				
severity	Severity of logs to be transferred to remote log server.	option	-	information																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.																							
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable comma-separated value (CSV) strings.</td></tr> <tr> <td><i>disable</i></td><td>Disable comma-separated value (CSV) strings.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable comma-separated value (CSV) strings.	<i>disable</i>	Disable comma-separated value (CSV) strings.																	
Option	Description																							
<i>enable</i>	Enable comma-separated value (CSV) strings.																							
<i>disable</i>	Disable comma-separated value (CSV) strings.																							
facility	Facility to log to remote syslog server.	option	-	local7																				
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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 syslogd.</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>UUCP server messages.</td></tr> </tbody> </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 syslogd.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	UUCP server messages.			
Option	Description																							
<i>kernel</i>	Kernel messages.																							
<i>user</i>	Random user-level messages.																							
<i>mail</i>	Mail system.																							
<i>daemon</i>	System daemons.																							
<i>auth</i>	Security/authorization messages.																							
<i>syslog</i>	Messages generated internally by syslogd.																							
<i>lpr</i>	Line printer subsystem.																							
<i>news</i>	Network news subsystem.																							
<i>uucp</i>	UUCP server messages.																							

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		

config storm-control

Parameter	Description	Type	Size	Default
local-override	Enable to override global FortiSwitch storm control settings for this FortiSwitch.	option	-	disable
	Option	Description		
	<i>enable</i>	Override global storm control settings.		
	<i>disable</i>	Use global storm control settings.		
rate	Rate in packets per second at which storm traffic is controlled . Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000	500
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Drop unknown unicast traffic.		
	<i>disable</i>	Allow unknown unicast traffic.		
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Drop unknown multicast traffic.		
	<i>disable</i>	Allow unknown multicast traffic.		
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Drop broadcast traffic.		
	<i>disable</i>	Allow broadcast traffic.		

config mirror

Parameter	Description	Type	Size	Default
status	Active/inactive mirror configuration.	option	-	inactive
	Option	Description		
	<i>active</i>	Activate mirror configuration.		
	<i>inactive</i>	Deactivate mirror configuration.		
switching-packet	Enable/disable switching functionality when mirroring.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable switching functionality when mirroring.		
	<i>disable</i>	Disable switching functionality when mirroring.		
dst	Destination port.	string	Maximum length: 63	
src-ingress <name>	Source ingress interfaces. Interface name.	string	Maximum length: 79	
src-egress <name>	Source egress interfaces. Interface name.	string	Maximum length: 79	

config static-mac

Parameter	Description	Type	Size	Default
type	Type.	option	-	static
	Option	Description		
	static	Static MAC.		
	sticky	Sticky MAC.		
vlan	Vlan.	string	Maximum length: 15	
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
interface	Interface name.	string	Maximum length: 35	
description	Description.	string	Maximum length: 63	

config custom-command

Parameter	Description	Type	Size	Default
command-name	Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller custom-command.	string	Maximum length: 35	

config igmp-snooping

Parameter	Description	Type	Size	Default
local-override	Enable/disable overriding the global IGMP snooping configuration.	option	-	disable
	Option	Description		
	enable	Override the global IGMP snooping configuration.		
	disable	Use the global IGMP snooping configuration.		
aging-time	Maximum time to retain a multicast snooping entry for which no packets have been seen .	integer	Minimum value: 15 Maximum value: 3600	300
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable unknown multicast flooding.		
	<i>disable</i>	Disable unknown multicast flooding.		

config 802-1X-settings

Parameter	Description	Type	Size	Default
local override	Enable to override global 802.1X settings on individual FortiSwitches.	option	-	disable
	Option	Description		
	<i>enable</i>	Override global 802.1X settings.		
	<i>disable</i>	Use global 802.1X settings.		
link-down-auth	Authentication state to set if a link is down.	option	-	set-unauth
	Option	Description		
	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.		
	<i>no-action</i>	Interface reauthentication is not needed.		
reauth-period	Reauthentication time interval .	integer	Minimum value: 0 Maximum value: 1440	60
max-reauth-attempt	Maximum number of authentication attempts .	integer	Minimum value: 0 Maximum value: 15	3
tx-period	802.1X Tx period .	integer	Minimum value: 4 Maximum value: 60	30

config switch-controller switch-group

Configure FortiSwitch switch groups.

```
config switch-controller switch-group
  Description: Configure FortiSwitch switch groups.
  edit <name>
    set description {string}
    set fortilink {string}
```

```

        set members <switch-id1>, <switch-id2>, ...
    next
end

```

config switch-controller switch-group

Parameter	Description	Type	Size	Default
description	Optional switch group description.	string	Maximum length: 63	
fortilink	FortiLink interface to which switch group members belong.	string	Maximum length: 15	
members <switch- id>	FortiSwitch members belonging to this switch group. Managed device ID.	string	Maximum length: 79	

config switch-controller stp-settings

Configure FortiSwitch spanning tree protocol (STP).

```

config switch-controller stp-settings
    Description: Configure FortiSwitch spanning tree protocol (STP).
    set name {string}
    set revision {integer}
    set hello-time {integer}
    set forward-time {integer}
    set max-age {integer}
    set max-hops {integer}
    set pending-timer {integer}
end

```

config switch-controller stp-settings

Parameter	Description	Type	Size	Default
name	Name of global STP settings configuration.	string	Maximum length: 31	
revision	STP revision number .	integer	Minimum value: 0 Maximum value: 65535	0
hello-time	Period of time between successive STP frame Bridge Protocol Data Units .	integer	Minimum value: 1 Maximum value: 10	2

Parameter	Description	Type	Size	Default
forward-time	Period of time a port is in listening and learning state .	integer	Minimum value: 4 Maximum value: 30	15
max-age	Maximum time before a bridge port expires its configuration BPDU information .	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops between the root bridge and the furthest bridge .	integer	Minimum value: 1 Maximum value: 40	20
pending-timer	Pending time .	integer	Minimum value: 1 Maximum value: 15	4

config switch-controller stp-instance

Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.

```
config switch-controller stp-instance
  Description: Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.
  edit <id>
    set vlan-range <vlan-name1>, <vlan-name2>, ...
  next
end
```

config switch-controller stp-instance

Parameter	Description	Type	Size	Default
vlan-range <vlan- name>	Configure VLAN range for STP instance. VLAN name.	string	Maximum length: 79	

config switch-controller storm-control

Configure FortiSwitch storm control.

```
config switch-controller storm-control
  Description: Configure FortiSwitch storm control.
  set rate {integer}
  set unknown-unicast [enable|disable]
  set unknown-multicast [enable|disable]
  set broadcast [enable|disable]
```

end

config switch-controller storm-control

Parameter	Description	Type	Size	Default
rate	Rate in packets per second at which storm traffic is controlled . Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000	500
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable
Option		Description		
		<i>enable</i> Enable unknown unicast storm control.		
		<i>disable</i> Disable unknown unicast storm control.		
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable
Option		Description		
		<i>enable</i> Enable unknown multicast storm control.		
		<i>disable</i> Disable unknown multicast storm control.		
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable
Option		Description		
		<i>enable</i> Enable broadcast storm control.		
		<i>disable</i> Disable broadcast storm control.		

config switch-controller global

Configure FortiSwitch global settings.

```
config switch-controller global
  Description: Configure FortiSwitch global settings.
  set mac-aging-interval {integer}
  set https-image-push [enable|disable]
  set vlan-all-mode [all|defined]
  set vlan-optimization [enable|disable]
  set disable-discovery <name1>, <name2>, ...
  set mac-retention-period {integer}
  set default-virtual-switch-vlan {string}
  set dhcp-server-access-list [enable|disable]
  set log-mac-limit-violations [enable|disable]
  set mac-violation-timer {integer}
```

```

set sn-dns-resolution [enable|disable]
set mac-event-logging [enable|disable]
set bounce-quarantined-link [disable|enable]
set quarantine-mode [by-vlan|by-redirect]
set update-user-device {option1}, {option2}, ...
config custom-command
    Description: List of custom commands to be pushed to all FortiSwitches in the VDOM.
    edit <command-entry>
        set command-name {string}
    next
end
set fips-enforce [disable|enable]
end

```

config switch-controller global

Parameter	Description	Type	Size	Default						
mac-aging-interval	Time after which an inactive MAC is aged out .	integer	Minimum value: 10 Maximum value: 1000000	300						
https-image-push	Enable/disable image push to FortiSwitch using HTTPS.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable image push to FortiSwitch using HTTPS.</td></tr> <tr> <td><i>disable</i></td><td>Disable image push to FortiSwitch using HTTPS.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable image push to FortiSwitch using HTTPS.	<i>disable</i>	Disable image push to FortiSwitch using HTTPS.			
Option	Description									
<i>enable</i>	Enable image push to FortiSwitch using HTTPS.									
<i>disable</i>	Disable image push to FortiSwitch using HTTPS.									
vlan-all-mode	VLAN configuration mode, user-defined-vlans or all-possible-vlans.	option	-	defined						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>all</i></td><td>Include all possible VLANs (1-4093).</td></tr> <tr> <td><i>defined</i></td><td>Include user defined VLANs.</td></tr> </tbody> </table>	Option	Description	<i>all</i>	Include all possible VLANs (1-4093).	<i>defined</i>	Include user defined VLANs.			
Option	Description									
<i>all</i>	Include all possible VLANs (1-4093).									
<i>defined</i>	Include user defined VLANs.									
vlan-optimization	FortiLink VLAN optimization.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable VLAN optimization on FortiSwitch units for auto-generated trunks.</td></tr> <tr> <td><i>disable</i></td><td>Disable VLAN optimization on FortiSwitch units for auto-generated trunks.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable VLAN optimization on FortiSwitch units for auto-generated trunks.	<i>disable</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.			
Option	Description									
<i>enable</i>	Enable VLAN optimization on FortiSwitch units for auto-generated trunks.									
<i>disable</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.									
disable-discovery <name>	Prevent this FortiSwitch from discovering. Managed device ID.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default
mac-retention-period	Time in hours after which an inactive MAC is removed from client DB (0 = aged out based on mac-aging-interval).	integer	Minimum value: 0 Maximum value: 168	24
default-virtual-switch-vlan	Default VLAN for ports when added to the virtual-switch.	string	Maximum length: 15	
dhcp-server-access-list	Enable/disable DHCP snooping server access list.	option	-	disable
Option		Description		
		<i>enable</i> Enable DHCP server access list.		
		<i>disable</i> Disable DHCP server access list.		
log-mac-limit-violations	Enable/disable logs for Learning Limit Violations.	option	-	disable
Option		Description		
		<i>enable</i> Enable Learn Limit Violation.		
		<i>disable</i> Disable Learn Limit Violation.		
mac-violation-timer	Set timeout for Learning Limit Violations (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
sn-dns-resolution	Enable/disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	option	-	enable
Option		Description		
		<i>enable</i> Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.		
		<i>disable</i> Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.		
mac-event-logging	Enable/disable MAC address event logging.	option	-	disable
Option		Description		
		<i>enable</i> Enable MAC address event logging.		
		<i>disable</i> Disable MAC address event logging.		

Parameter	Description	Type	Size	Default												
bounce-quarantined-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last. Helps to re-initiate the DHCP process for a device.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr> <tr> <td><i>enable</i></td><td>Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.									
Option	Description															
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.															
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.															
quarantine-mode	Quarantine mode.	option	-	by-vlan												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>by-vlan</i></td><td>Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.</td></tr> <tr> <td><i>by-redirect</i></td><td>Quarantined device traffic is redirected only to the FortiGate on the received VLAN.</td></tr> </tbody> </table>	Option	Description	<i>by-vlan</i>	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.	<i>by-redirect</i>	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.									
Option	Description															
<i>by-vlan</i>	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.															
<i>by-redirect</i>	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.															
update-user-device	Control which sources update the device user list.	option	-	mac-cache lldp dhcp-snooping l2-db l3-db												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>mac-cache</i></td><td>Update MAC address from switch-controller mac-cache.</td></tr> <tr> <td><i>lldp</i></td><td>Update from FortiSwitch LLDP neighbor database.</td></tr> <tr> <td><i>dhcp-snooping</i></td><td>Update from FortiSwitch DHCP snooping client and server databases.</td></tr> <tr> <td><i>l2-db</i></td><td>Update from FortiSwitch Network-monitor Layer 2 tracking database.</td></tr> <tr> <td><i>l3-db</i></td><td>Update from FortiSwitch Network-monitor Layer 3 tracking database.</td></tr> </tbody> </table>	Option	Description	<i>mac-cache</i>	Update MAC address from switch-controller mac-cache.	<i>lldp</i>	Update from FortiSwitch LLDP neighbor database.	<i>dhcp-snooping</i>	Update from FortiSwitch DHCP snooping client and server databases.	<i>l2-db</i>	Update from FortiSwitch Network-monitor Layer 2 tracking database.	<i>l3-db</i>	Update from FortiSwitch Network-monitor Layer 3 tracking database.			
Option	Description															
<i>mac-cache</i>	Update MAC address from switch-controller mac-cache.															
<i>lldp</i>	Update from FortiSwitch LLDP neighbor database.															
<i>dhcp-snooping</i>	Update from FortiSwitch DHCP snooping client and server databases.															
<i>l2-db</i>	Update from FortiSwitch Network-monitor Layer 2 tracking database.															
<i>l3-db</i>	Update from FortiSwitch Network-monitor Layer 3 tracking database.															
fips-enforce	Enable/disable enforcement of FIPS on managed FortiSwitch devices.	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable enforcement of FIPS on managed FortiSwitch devices.</td></tr> <tr> <td><i>enable</i></td><td>Enable enforcement of FIPS on managed FortiSwitch devices.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable enforcement of FIPS on managed FortiSwitch devices.	<i>enable</i>	Enable enforcement of FIPS on managed FortiSwitch devices.									
Option	Description															
<i>disable</i>	Disable enforcement of FIPS on managed FortiSwitch devices.															
<i>enable</i>	Enable enforcement of FIPS on managed FortiSwitch devices.															

config custom-command

Parameter	Description	Type	Size	Default
command-name	Name of custom command to push to all FortiSwitches in VDOM.	string	Maximum length: 35	

config switch-controller system

Configure system-wide switch controller settings.

```
config switch-controller system
  Description: Configure system-wide switch controller settings.
  set parallel-process-override [disable|enable]
  set parallel-process {integer}
  set data-sync-interval {integer}
  set iot-weight-threshold {integer}
  set iot-scan-interval {integer}
  set iot-holdoff {integer}
  set iot-mac-idle {integer}
  set nac-periodic-interval {integer}
  set dynamic-periodic-interval {integer}
  set tunnel-mode [compatible|strict]
end
```

config switch-controller system

Parameter	Description	Type	Size	Default
parallel-process-override	Enable/disable parallel process override.	option	-	disable
Option		Description		
		disable Disable maximum parallel process override.		
		enable Enable maximum parallel process override.		
parallel-process	Maximum number of parallel processes.	integer	Minimum value: 1 Maximum value: 32 **	1
data-sync-interval	Time interval between collection of switch data .	integer	Minimum value: 30 Maximum value: 1800	60

Parameter	Description	Type	Size	Default
iot-weight-threshold	MAC entry's confidence value. Value is re-queried when below this value .	integer	Minimum value: 0 Maximum value: 255	1
iot-scan-interval	IoT scan interval .	integer	Minimum value: 2 Maximum value: 10080	60
iot-holdoff	MAC entry's creation time. Time must be greater than this value for an entry to be created .	integer	Minimum value: 0 Maximum value: 10080	5
iot-mac-idle	MAC entry's idle time. MAC entry is removed after this value .	integer	Minimum value: 0 Maximum value: 10080	1440
nac-periodic-interval	Periodic time interval to run NAC engine .	integer	Minimum value: 5 Maximum value: 60	15
dynamic-periodic-interval	Periodic time interval to run Dynamic port policy engine .	integer	Minimum value: 5 Maximum value: 60	15
tunnel-mode	Compatible/strict tunnel mode.	option	-	compatible
Option	Description			
<i>compatible</i>	Allow for backward compatible ciphers.			
<i>strict</i>	Follow system.strong-crypto ciphers.			

** Values may differ between models.

config switch-controller switch-log

Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log).

```
config switch-controller switch-log
  Description: Configure FortiSwitch logging (logs are transferred to and inserted into
               FortiGate event log).
  set status [enable|disable]
  set severity [emergency|alert|...]
```

end

config switch-controller switch-log

Parameter	Description	Type	Size	Default
status	Enable/disable adding FortiSwitch logs to FortiGate event log.	option	-	enable
Option		Description		
		<i>enable</i> Add FortiSwitch logs to FortiGate event log.		
		<i>disable</i> Do not add FortiSwitch logs to FortiGate event log.		
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	notification
Option		Description		
		<i>emergency</i> Emergency level.		
		<i>alert</i> Alert level.		
		<i>critical</i> Critical level.		
		<i>error</i> Error level.		
		<i>warning</i> Warning level.		
		<i>notification</i> Notification level.		
		<i>information</i> Information level.		
		<i>debug</i> Debug level.		

config switch-controller igmp-snooping

Configure FortiSwitch IGMP snooping global settings.

```
config switch-controller igmp-snooping
  Description: Configure FortiSwitch IGMP snooping global settings.
  set aging-time {integer}
  set flood-unknown-multicast [enable|disable]
end
```

config switch-controller igmp-snooping

Parameter	Description	Type	Size	Default
aging-time	Maximum number of seconds to retain a multicast snooping entry for which no packets have been seen .	integer	Minimum value: 15 Maximum value: 3600	300
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable
Option	Description			
<i>enable</i>	Enable unknown multicast flooding.			
<i>disable</i>	Disable unknown multicast flooding.			

config switch-controller sflow

Configure FortiSwitch sFlow.

```
config switch-controller sflow
  Description: Configure FortiSwitch sFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
end
```

config switch-controller sflow

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0
collector-port	SFlow collector port .	integer	Minimum value: 0 Maximum value: 65535	6343

config switch-controller quarantine

Configure FortiSwitch quarantine support.

```
config switch-controller quarantine
  Description: Configure FortiSwitch quarantine support.
  set quarantine [enable|disable]
  config targets
    Description: Quarantine MACs.
```

```

edit <mac>
    set description {string}
    set tag <tags1>, <tags2>, ...
next
end
end

```

config switch-controller quarantine

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

config targets

Parameter	Description	Type	Size	Default
description	Description for the quarantine MAC.	string	Maximum length: 63	
tag <tags>	Tags for the quarantine MAC. Tag string(e.g. string1 string2 string3).	string	Maximum length: 63	

config switch-controller network-monitor-settings

Configure network monitor settings.

```

config switch-controller network-monitor-settings
    Description: Configure network monitor settings.
        set network-monitoring [enable|disable]
end

```

config switch-controller network-monitor-settings

Parameter	Description	Type	Size	Default
network-monitoring	Enable/disable passive gathering of information by FortiSwitch units concerning other network devices.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable network monitoring on FortiSwitch.		
	<i>disable</i>	Disable network monitoring on FortiSwitch.		

config switch-controller flow-tracking

Configure FortiSwitch flow tracking and export via ipfix/netflow.

```
config switch-controller flow-tracking
    Description: Configure FortiSwitch flow tracking and export via ipfix/netflow.
    set sample-mode {local|perimeter|...}
    set sample-rate {integer}
    set format {netflow1|netflow5|...}
    set collector-ip {ipv4-address}
    set collector-port {integer}
    set transport {udp|tcp|...}
    set level {vlan|ip|...}
    set max-export-pkt-size {integer}
    set timeout-general {integer}
    set timeout-icmp {integer}
    set timeout-max {integer}
    set timeout-tcp {integer}
    set timeout-tcp-fin {integer}
    set timeout-tcp-rst {integer}
    set timeout-udp {integer}
    config aggregates
        Description: Configure aggregates in which all traffic sessions matching the IP Address
                     will be grouped into the same flow.
        edit <id>
            set ip {ipv4-classnet}
        next
    end
end
```

config switch-controller flow-tracking

Parameter	Description	Type	Size	Default	
sample-mode	Configure sample mode for the flow tracking.	option	-	perimeter	
Parameter	Description	Option	Size	Default	
sample-mode	Configure sample mode for the flow tracking.	local perimeter device-ingress	Set local mode which samples on the specific switch port. Set perimeter mode which samples on all switch fabric ports and fortiflink port at the ingress. Set device -ingress mode which samples across all switch ports at the ingress.	-	perimeter
sample-rate	Configure sample rate for the perimeter and device-ingress sampling.	integer	Minimum value: 0 Maximum value: 99999	512	
format	Configure flow tracking protocol.	option	-	netflow9	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>netflow1</i>	Netflow version 1 sampling.		
	<i>netflow5</i>	Netflow version 5 sampling.		
	<i>netflow9</i>	Netflow version 9 sampling.		
	<i>ipfix</i>	Ipfix sampling.		
collector-ip	Configure collector ip address.	ipv4-address	Not Specified	0.0.0.0
collector-port	Configure collector port number.	integer	Minimum value: 0 Maximum value: 65535	0
transport	Configure L4 transport protocol for exporting packets.	option	-	udp
	Option	Description		
	<i>udp</i>	UDP protocol.		
	<i>tcp</i>	TCP protocol.		
	<i>sctp</i>	SCTP protocol.		
level	Configure flow tracking level.	option	-	ip
	Option	Description		
	<i>vlan</i>	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.		
	<i>ip</i>	Collects srcip/dstip from the sample packet.		
	<i>port</i>	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.		
	<i>proto</i>	Collects srcip/dstip/protocol from the sample packet.		
	<i>mac</i>	Collects smac/dmac from the sample packet.		
max-export-pkt-size	Configure flow max export packet size .	integer	Minimum value: 512 Maximum value: 9216	512
timeout-general	Configure flow session general timeout .	integer	Minimum value: 60 Maximum value: 604800	3600

Parameter	Description	Type	Size	Default
timeout-icmp	Configure flow session ICMP timeout .	integer	Minimum value: 60 Maximum value: 604800	300
timeout-max	Configure flow session max timeout .	integer	Minimum value: 60 Maximum value: 604800	604800
timeout-tcp	Configure flow session TCP timeout .	integer	Minimum value: 60 Maximum value: 604800	3600
timeout-tcp-fin	Configure flow session TCP FIN timeout .	integer	Minimum value: 60 Maximum value: 604800	300
timeout-tcp-rst	Configure flow session TCP RST timeout .	integer	Minimum value: 60 Maximum value: 604800	120
timeout-udp	Configure flow session UDP timeout .	integer	Minimum value: 60 Maximum value: 604800	300

config aggregates

Parameter	Description	Type	Size	Default
ip	IP address to group all matching traffic sessions to a flow.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config switch-controller snmp-sysinfo

Configure FortiSwitch SNMP system information globally.

```
config switch-controller snmp-sysinfo
  Description: Configure FortiSwitch SNMP system information globally.
  set status [disable|enable]
  set engine-id {string}
  set description {string}
  set contact-info {string}
  set location {string}
end
```

config switch-controller snmp-sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SNMP.		
	<i>enable</i>	Enable SNMP.		
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24	
description	System description.	string	Maximum length: 35	
contact-info	Contact information.	string	Maximum length: 35	
location	System location.	string	Maximum length: 35	

config switch-controller snmp-trap-threshold

Configure FortiSwitch SNMP trap threshold values globally.

```
config switch-controller snmp-trap-threshold
  Description: Configure FortiSwitch SNMP trap threshold values globally.
  set trap-high-cpu-threshold {integer}
  set trap-low-memory-threshold {integer}
  set trap-log-full-threshold {integer}
end
```

config switch-controller snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80

Parameter	Description	Type	Size	Default
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90

config switch-controller snmp-community

Configure FortiSwitch SNMP v1/v2c communities globally.

```
config switch-controller snmp-community
  Description: Configure FortiSwitch SNMP v1/v2c communities globally.
  edit <id>
    set name {string}
    set status [disable|enable]
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ip {user}
      next
    end
    set query-v1-status [disable|enable]
    set query-v1-port {integer}
    set query-v2c-status [disable|enable]
    set query-v2c-port {integer}
    set trap-v1-status [disable|enable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v2c-status [disable|enable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set events {option1}, {option2}, ...
  next
end
```

config switch-controller snmp-community

Parameter	Description	Type	Size	Default
name	SNMP community name.	string	Maximum length: 35	
status	Enable/disable this SNMP community.	option	-	enable
Option		Description		
		disable Disable SNMP community.		
		enable Enable SNMP community.		

Parameter	Description	Type	Size	Default
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v1 queries.		
	<i>enable</i>	Enable SNMP v1 queries.		
query-v1-port	SNMP v1 query port .	integer	Minimum value: 0 Maximum value: 65535	161
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v2c queries.		
	<i>enable</i>	Enable SNMP v2c queries.		
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535	161
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP v1 traps.		
	<i>enable</i>	Enable SNMP v1 traps.		
trap-v1-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable SNMP v2c traps.		
	<i>enable</i>	Enable SNMP v2c traps.		
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip ent-conf-change
	Option	Description		
	<i>cpu-high</i>	Send a trap when CPU usage too high.		
	<i>mem-low</i>	Send a trap when available memory is low.		
	<i>log-full</i>	Send a trap when log disk space becomes low.		
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		

config hosts

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

config switch-controller snmp-user

Configure FortiSwitch SNMP v3 users globally.

```
config switch-controller snmp-user
  Description: Configure FortiSwitch SNMP v3 users globally.
  edit <name>
    set queries {disable|enable}
    set query-port {integer}
```

```

set security-level [no-auth-no-priv|auth-no-priv|...]
set auth-proto [md5|sha1|...]
set auth-pwd {password}
set priv-proto [aes128|aes192|...]
set priv-pwd {password}
next
end

```

config switch-controller snmp-user

Parameter	Description	Type	Size	Default
queries	Enable/disable SNMP queries for this user.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable SNMP queries for this user.		
	<i>enable</i>	Enable SNMP queries for this user.		
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161
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	-	sha256
	Option	Description		
	<i>md5</i>	HMAC-MD5-96 authentication protocol.		
	<i>sha1</i>	HMAC-SHA-1 authentication protocol.		
	<i>sha224</i>	HMAC-SHA-224 authentication protocol.		
	<i>sha256</i>	HMAC-SHA-256 authentication protocol.		
	<i>sha384</i>	HMAC-SHA-384 authentication protocol.		
	<i>sha512</i>	HMAC-SHA-512 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	

Parameter	Description	Type	Size	Default
priv-proto	Privacy (encryption) protocol.	option	-	aes128
Option	Description			
aes128	CFB128-AES-128 symmetric encryption protocol.			
aes192	CFB128-AES-192 symmetric encryption protocol.			
aes192c	CFB128-AES-192-C symmetric encryption protocol.			
aes256	CFB128-AES-256 symmetric encryption protocol.			
aes256c	CFB128-AES-256-C symmetric encryption protocol.			
des	CBC-DES symmetric encryption protocol.			
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

config switch-controller traffic-sniffer

Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.

```

config switch-controller traffic-sniffer
    Description: Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.
    set mode [erspan-auto|rspan|...]
    set erspan-ip {ipv4-address}
    config target-mac
        Description: Sniffer MACs to filter.
        edit <mac>
            set description {string}
        next
    end
    config target-ip
        Description: Sniffer IPs to filter.
        edit <ip>
            set description {string}
        next
    end
    config target-port
        Description: Sniffer ports to filter.
        edit <switch-id>
            set description {string}
            set in-ports <name1>, <name2>, ...
            set out-ports <name1>, <name2>, ...
        next
    end
end

```

config switch-controller traffic-sniffer

Parameter	Description	Type	Size	Default
mode	Configure traffic sniffer mode.	option	-	erspan-auto
	Option Description			
erspan-auto Mirror traffic using a GRE tunnel.				
rspan Mirror traffic on a layer2 VLAN.				
none Disable traffic mirroring (sniffer).				
erspan-ip	Configure ERSPAN collector IP address.	ipv4-address	Not Specified	0.0.0.0

config target-mac

Parameter	Description	Type	Size	Default
description	Description for the sniffer MAC.	string	Maximum length: 63	

config target-ip

Parameter	Description	Type	Size	Default
description	Description for the sniffer IP.	string	Maximum length: 63	

config target-port

Parameter	Description	Type	Size	Default
description	Description for the sniffer port entry.	string	Maximum length: 63	
in-ports <name>	Configure source ingress port interfaces. Interface name.	string	Maximum length: 79	
out-ports <name>	Configure source egress port interfaces. Interface name.	string	Maximum length: 79	

config switch-controller remote-log

Configure logging by FortiSwitch device to a remote syslog server.

```
config switch-controller remote-log
```

```
    Description: Configure logging by FortiSwitch device to a remote syslog server.  
    edit <name>
```

```

set status [enable|disable]
set server {string}
set port {integer}
set severity [emergency|alert|...]
set csv [enable|disable]
set facility [kernel|user|...]
next
end

```

config switch-controller remote-log

Parameter	Description	Type	Size	Default
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.		
	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.		
server	IPv4 address of the remote syslog server.	string	Maximum length: 63	
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514
severity	Severity of logs to be transferred to remote log server.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable comma-separated value (CSV) strings.		
	<i>disable</i>	Disable comma-separated value (CSV) strings.		
facility	Facility to log to remote syslog server.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslogd.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	UUCP server messages.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		
	<i>local4</i>	Reserved for local use.		
	<i>local5</i>	Reserved for local use.		
	<i>local6</i>	Reserved for local use.		
	<i>local7</i>	Reserved for local use.		

config switch-controller mac-policy

Configure MAC policy to be applied on the managed FortiSwitch devices through NAC device.

```
config switch-controller mac-policy
    Description: Configure MAC policy to be applied on the managed FortiSwitch devices through
                 NAC device.
    edit <name>
        set description {string}
        set fortilink {string}
        set vlan {string}
        set traffic-policy {string}
        set count [disable|enable]
        set bounce-port-link [disable|enable]
    next
end
```

config switch-controller mac-policy

Parameter	Description	Type	Size	Default
description	Description for the MAC policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this MAC policy belongs to.	string	Maximum length: 15	
vlan	Ingress traffic VLAN assignment for the MAC address matching this MAC policy.	string	Maximum length: 15	
traffic-policy	Traffic policy to be applied when using this MAC policy.	string	Maximum length: 63	
count	Enable/disable packet count on the NAC device.	option	-	disable
Option	Description			
<i>disable</i>	Enable packet count on the NAC device.			
<i>enable</i>	Disable packet count on the NAC device.			
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.	option	-	enable
Option	Description			
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.			
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.			

system

This section includes syntax for the following commands:

- [config system replacemsg-image on page 1013](#)
- [config system ips-urlfilter-dns6 on page 1099](#)
- [config system ipv6-tunnel on page 1096](#)
- [config system autoupdate tunneling on page 1051](#)
- [config system replacemsg utm on page 1023](#)
- [config system ip-conflict status on page 1191](#)
- [config system modem on page 1068](#)
- [config system dns on page 1002](#)
- [config system dhcp6 server on page 1064](#)
- [config system proxy-arp on page 1170](#)
- [config system performance status on page 1076](#)
- [config system dedicated-mgmt on page 1000](#)
- [config system source-ip status on page 1190](#)
- [config system geoip-override on page 1192](#)
- [config system central-mgmt on page 1078](#)
- [config system acme on page 1232](#)
- [config system dns64 on page 1188](#)
- [config system ha-monitor on page 998](#)
- [config system snmp community on page 1038](#)
- [config system alarm on page 1165](#)
- [config system replacemsg admin on page 1019](#)
- [config system ddns on page 1005](#)
- [config system fortisandbox on page 1193](#)
- [config system gre-tunnel on page 1121](#)
- [config system replacemsg mail on page 1014](#)
- [config system ha on page 987](#)
- [config system fortiguard-log-service on page 1078](#)
- [config system fortiguard-service on page 1077](#)
- [config system sms-server on page 956](#)
- [config system sflow on page 1007](#)
- [config system mobile-tunnel on page 1125](#)
- [config system automation-action on page 1205](#)
- [config system api-user on page 963](#)
- [config system network-visibility on page 1099](#)
- [config system automation-stitch on page 1210](#)
- [config system csf on page 1197](#)
- [config system vdom on page 844](#)
- [config system virtual-switch on page 949](#)
- [config system sso-forticloud-admin on page 965](#)

-
- config system vdom-exception on page 1196
 - config system session-ttl on page 1052
 - config system replacemsg icap on page 1024
 - config system dhcp server on page 1053
 - config system central-management on page 1084
 - config system password-policy on page 952
 - config system session-info ttl on page 1191
 - config system accprofile on page 882
 - config system vdom-sflow on page 1008
 - config system auto-update status on page 1190
 - config system password-policy-guest-admin on page 954
 - config system settings on page 966
 - config system global on page 845
 - config system automation-destination on page 1210
 - config system session-info statistics on page 1191
 - config system speed-test-server on page 1141
 - config system replacemsg sslvpn on page 1021
 - config system session-helper on page 1169
 - config system vxlan on page 1129
 - config system dscp-based-priority on page 1172
 - config system ips-urlfilter-dns on page 1098
 - config system ipsec-aggregate on page 1123
 - config system startup-error-log on page 1190
 - config system ha-nonsync-csum on page 1078
 - config system mac-address-table on page 1168
 - config system vdom-link on page 897
 - config system ptp on page 1183
 - config system interface on page 902
 - config system session-info list on page 1190
 - config system alias on page 1078
 - config system snmp sysinfo on page 1037
 - config system lte-modem on page 901
 - config system switch-interface on page 898
 - config system speed-test-schedule on page 1149
 - config system auto-update versions on page 1190
 - config system cmdb on page 1077
 - config system physical-switch on page 949
 - config system arp-table on page 1001
 - config system auto-script on page 1078
 - config system ipv6-neighbor-cache on page 1002
 - config system checksum status on page 1077
 - config system arp on page 1163
 - config system fortiguard on page 1155
 - config system autoupdate schedule on page 1050
 - config system tos-based-priority on page 1171

-
- config system object-tagging on page 899
 - config system zone on page 1088
 - config system performance firewall packet-distribution on page 1076
 - config system sdn-connector on page 1089
 - config system probe-response on page 1173
 - config system 3g-modem custom on page 1075
 - config system replacemsg http on page 1015
 - config system saml on page 1212
 - config system vne-tunnel on page 1217
 - config system pppoe-interface on page 1127
 - config system virtual-wire-pair on page 1131
 - config system session-info expectation on page 1191
 - config system geneve on page 1130
 - config system ftm-push on page 1192
 - config system fortiai on page 1195
 - config system auto-install on page 1179
 - config system nd-proxy on page 1211
 - config system performance firewall statistics on page 1076
 - config system session-info full-stat on page 1191
 - config system federated-upgrade on page 1215
 - config system ike on page 1218
 - config system mgmt-csum on page 1077
 - config system replacemsg traffic-quota on page 1023
 - config system fortimanager on page 1081
 - config system session-helper-info list on page 1191
 - config system replacemsg nac-quar on page 1022
 - config system replacemsg spam on page 1018
 - config system fortianalyzer-connectivity on page 1077
 - config system ipip-tunnel on page 1124
 - config system replacemsg-group on page 1026
 - config system replacemsg automation on page 1025
 - config system session6 on page 1077
 - config system vdom-property on page 1139
 - config system vdom-netflow on page 1011
 - config system info admin ssh on page 1080
 - config system lldp network-policy on page 1142
 - config system vdom-radius-server on page 1189
 - config system storage on page 999
 - config system admin on page 957
 - config system sso-admin on page 965
 - config system ntp on page 1181
 - config system standalone-cluster on page 1151
 - config system fssso-polling on page 986
 - config system sit-tunnel on page 985
 - config system replacemsg ftp on page 1016

-
- config system stp on page 951
 - config system replacemsg webproxy on page 1015
 - config system geoip-country on page 1089
 - config system console on page 1179
 - config system info admin status on page 1079
 - config system link-monitor on page 1174
 - config system email-server on page 1163
 - config system replacemsg fortiguard-wf on page 1017
 - config system resource-limits on page 1136
 - config system management-tunnel on page 1080
 - config system fips-cc on page 1170
 - config system ips on page 1162
 - config system fm on page 1083
 - config system snmp user on page 1045
 - config system custom-language on page 956
 - config system automation-trigger on page 1201
 - config system wccp on page 1185
 - config system status on page 1075
 - config system npu on page 892
 - config system sdwan on page 1101
 - config system netflow on page 1009
 - config system dns-server on page 1135
 - config system dns-database on page 1132
 - config system replacemsg auth on page 1020
 - config system external-resource on page 1097
 - config system cluster-sync on page 1152
 - config system session on page 1076
 - config system vdom-dns on page 1012
 - config system replacemsg alertmail on page 1019
 - config system performance top on page 1076

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
short-name	VDOM short name.	string	Maximum length: 11	
vcluster-id	Virtual cluster ID .	integer	Minimum value: 0 Maximum value: 4294967295	0
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295	0

config system global

Configure global attributes.

```
config system global
  Description: Configure global attributes.
  set language [english|french|...]
  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-wireless-opensecurity [enable|disable]
  set gui-display-hostname [enable|disable]
  set gui-fortigate-cloud-sandbox [enable|disable]
  set gui-firmware-upgrade-warning [enable|disable]
  set gui-allow-default-hostname [enable|disable]
  set gui-forticare-registration-setup-warning [enable|disable]
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admintimeout {integer}
  set admin-console-timeout {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 daily-restart [enable|disable]
  set restart-time {user}
  set radius-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 dst [enable|disable]
set timezone [01|02|...]
set traffic-priority [tos|dscp]
set traffic-priority-level [low|medium|...]
set anti-replay [disable|loose|...]
set send-pmtu-icmp [enable|disable]
set honor-df [enable|disable]
set pmtu-discovery [enable|disable]
set virtual-switch-vlan [enable|disable]
set revision-image-auto-backup [enable|disable]
set revision-backup-on-logout [enable|disable]
set management-vdom {string}
set hostname {string}
set alias {string}
set strong-crypto [enable|disable]
set ssh-cbc-cipher [enable|disable]
set ssh-hmac-md5 [enable|disable]
set ssh-kex-sha1 [enable|disable]
set ssh-mac-weak [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-re-authentication-mode [session|traffic|...]
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
set proxy-resource-mode [enable|disable]
set sys-perf-log-interval {integer}
set check-protocol-header [loose|strict]
set vip-arp-range [unlimited|restricted]
set reset-sessionless-tcp [enable|disable]
set allow-traffic-redirect [enable|disable]
set ipv6-allow-traffic-redirect [enable|disable]
set strict-dirty-session-check [enable|disable]
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 memory-use-threshold-extreme {integer}
set memory-use-threshold-red {integer}
```

```
set memory-use-threshold-green {integer}
set cpu-use-threshold {integer}
set check-reset-range [strict|disable]
set vdom-mode [no-vdom|split-vdom|...]
set long-vdom-name [enable|disable]
set edit-vdom-prompt [enable|disable]
set admin-port {integer}
set admin-sport {integer}
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 default-service-source-port {user}
set admin-maintainer [enable|disable]
set admin-reset-button [enable|disable]
set admin-server-cert {string}
set user-server-cert {string}
set admin-https-pki-required [enable|disable]
set wifi-certificate {string}
set wifi-ca-certificate {string}
set auth-http-port {integer}
set auth-https-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-result-submission [enable|disable]
set security-rating-run-on-schedule [enable|disable]
set wireless-controller [enable|disable]
set wireless-controller-port {integer}
set fortiextender-data-port {integer}
set fortiextender [disable|enable]
set fortiextender-vlan-mode [enable|disable]
set switch-controller [disable|enable]
set switch-controller-reserved-network {ipv4-classnet-host}
set dnsproxy-worker-count {integer}
set url-filter-count {integer}
set proxy-worker-count {integer}
set scanunit-count {integer}
set proxy-hardware-acceleration [disable|enable]
set fgd-alert-subscription {option1}, {option2}, ...
set ipsec-hmac-offload [enable|disable]
set ipv6-accept-dad {integer}
set ipv6-allow-anycast-probe [enable|disable]
set csr-ca-attribute [enable|disable]
```

```
set wimax-4g-usb [enable|disable]
set cert-chain-max {integer}
set sslvpn-max-worker-count {integer}
set sslvpn-kxp-hardware-acceleration [enable|disable]
set sslvpn-cipher-hardware-acceleration [enable|disable]
set sslvpn-ems-sn-check [enable|disable]
set sslvpn-plugin-version-check [enable|disable]
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 wad-worker-count {integer}
set wad-csvc-cs-count {integer}
set wad-csvc-db-count {integer}
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 arp-max-entry {integer}
set ha-affinity {string}
set cmdbsvr-affinity {string}
set ndp-max-entry {integer}
set br-fdb-max-entry {integer}
set max-route-cache-size {integer}
set ipsec-asic-offload [enable|disable]
set ipsec-soft-dec-async [enable|disable]
set device-idle-timeout {integer}
set user-device-store-max-devices {integer}
set user-device-store-max-users {integer}
set gui-device-latitude {string}
set gui-device-longitude {string}
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 legacy-poe-device-support [enable|disable]
set cloud-communication [enable|disable]
set fec-port {integer}
set ipsec-ha-seqjump-rate {integer}
set fortitoken-cloud [enable|disable]
set faz-disk-buffer-size {integer}
set irq-time-accounting [auto|force]
set fortiipam-integration [enable|disable]
set management-ip {string}
set management-port {integer}
set management-port-use-admin-sport [enable|disable]
end
```

config system global

Parameter	Description	Type	Size	Default
language	GUI display language.	option	-	english
	Option	Description		
	<i>english</i>	English.		
	<i>french</i>	French.		
	<i>spanish</i>	Spanish.		
	<i>portuguese</i>	Portuguese.		
	<i>japanese</i>	Japanese.		
	<i>trach</i>	Traditional Chinese.		
	<i>simch</i>	Simplified Chinese.		
	<i>korean</i>	Korean.		
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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-wireless-opensecurity	Enable/disable wireless open security option 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-display-hostname	Enable/disable displaying the FortiGate's hostname on the GUI login page.	option	-	disable
	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 FortiGate 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-allow-default-hostname	Enable/disable the factory default hostname warning on the GUI setup wizard.	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-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.		
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.		
admintimeout	Number of minutes before an idle administrator session times out . A shorter idle timeout is more secure.	integer	Minimum value: 1 Maximum value: 480	5
admin-console-timeout	Console login timeout that overrides the admintimeout value . 0 the default, disables this timeout.	integer	Minimum value: 15 Maximum value: 300	0
admin-concurrent	Enable/disable concurrent administrator logins. (Use policy-auth-concurrent for firewall authenticated users.)	option	-	enable
	Option	Description		
	<i>enable</i>	Enable admin concurrent login.		
	<i>disable</i>	Disable admin concurrent login.		
admin-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

Parameter	Description	Type	Size	Default
admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 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
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295	5
daily-restart	Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.	option	-	disable
Option	Description			
<i>enable</i>	Enable daily reboot of the FortiGate.			
<i>disable</i>	Disable daily reboot of the FortiGate.			
restart-time	Daily restart time (hh:mm).	user	Not Specified	
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812
admin-login-max	Maximum number of administrators who can be logged in at the same time	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.	integer	Minimum value: 1 Maximum value: 300	5

Parameter	Description	Type	Size	Default												
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds .	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												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable batch mode to execute in CMDB server.</td></tr> <tr> <td><i>disable</i></td><td>Disable batch mode to execute in CMDB server.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable batch mode to execute in CMDB server.	<i>disable</i>	Disable batch mode to execute in CMDB server.									
Option	Description															
<i>enable</i>	Enable batch mode to execute in CMDB server.															
<i>disable</i>	Disable batch mode to execute in CMDB server.															
multi-factor-authentication	Enforce all login methods to require an additional authentication factor .	option	-	optional												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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-minproto-version	Minimum supported protocol version for SSL/TLS connections .	option	-	TLSv1-2												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.															
dst	Enable/disable daylight saving time.	option	-	enable												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable daylight saving time.		
	<i>disable</i>	Disable daylight saving time.		
timezone	Number corresponding to your time zone from 00 to 86. Enter set timezone ? to view the list of time zones and the numbers that represent them.	option	-	00
	Option	Description		
	01	(GMT-11:00) Midway Island, Samoa		
	02	(GMT-10:00) Hawaii		
	03	(GMT-9:00) Alaska		
	04	(GMT-8:00) Pacific Time (US & Canada)		
	05	(GMT-7:00) Arizona		
	81	(GMT-7:00) Baja California Sur, Chihuahua		
	06	(GMT-7:00) Mountain Time (US & Canada)		
	07	(GMT-6:00) Central America		
	08	(GMT-6:00) Central Time (US & Canada)		
	09	(GMT-6:00) Mexico City		
	10	(GMT-6:00) Saskatchewan		
	11	(GMT-5:00) Bogota, Lima, Quito		
	12	(GMT-5:00) Eastern Time (US & Canada)		
	13	(GMT-5:00) Indiana (East)		
	74	(GMT-4:00) Caracas		
	14	(GMT-4:00) Atlantic Time (Canada)		
	77	(GMT-4:00) Georgetown		
	15	(GMT-4:00) La Paz		
	87	(GMT-4:00) Paraguay		
	16	(GMT-3:00) Santiago		
	17	(GMT-3:30) Newfoundland		
	18	(GMT-3:00) Brasilia		
	19	(GMT-3:00) Buenos Aires		

Parameter	Description	Type	Size	Default
	Option	Description		
	20	(GMT-3:00) Nuuk (Greenland)		
	75	(GMT-3:00) Uruguay		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Athens, Sofia, Vilnius		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		

Parameter	Description	Type	Size	Default
	Option	Description		
	43	(GMT+4:00) Baku		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	44	(GMT+4:30) Kabul		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepura		
	48	(GMT+5:45) Kathmandu		
	45	(GMT+5:00) Ekaterinburg		
	49	(GMT+6:00) Almaty, Novosibirsk		
	50	(GMT+6:00) Astana, Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		
	58	(GMT+8:00) Perth		
	59	(GMT+8:00) Taipei		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul		
	62	(GMT+9:30) Adelaide		
	63	(GMT+9:30) Darwin		
	61	(GMT+9:00) Yakutsk		
	64	(GMT+10:00) Brisbane		
	65	(GMT+10:00) Canberra, Melbourne, Sydney		
	66	(GMT+10:00) Guam, Port Moresby		
	67	(GMT+10:00) Hobart		
	68	(GMT+10:00) Vladivostok		
	69	(GMT+10:00) Magadan		
	70	(GMT+11:00) Solomon Is., New Caledonia		

Parameter	Description	Type	Size	Default
	Option	Description		
	71	(GMT+12:00) Auckland, Wellington		
	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.		
	00	(GMT+12:00) Eniwetok, Kwajalein		
	82	(GMT+12:45) Chatham Islands		
	73	(GMT+13:00) Nuku'alofa		
	86	(GMT+13:00) Samoa		
	76	(GMT+14:00) Kiribati		
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos
	Option	Description		
	<i>tos</i>	IP TOS.		
	<i>dscp</i>	DSCP (DiffServ) DS.		
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-	medium
	Option	Description		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-	strict
	Option	Description		
	<i>disable</i>	Disable anti-replay check.		
	<i>loose</i>	Loose anti-replay check.		
	<i>strict</i>	Strict anti-replay check.		
send-pmtu-icmp	Enable/disable sending of path maximum transmission unit (PMTU) - ICMP destination unreachable packet and to support PMTUD protocol on your network to reduce fragmentation of packets.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.		
	<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.		
honor-df	Enable/disable honoring of Don't-Fragment (DF) flag.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable honoring of Don't-Fragment flag.		
	<i>disable</i>	Disable honoring of Don't-Fragment flag.		
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable path MTU discovery.		
	<i>disable</i>	Disable path MTU discovery.		
virtual-switch-vlan *	Enable/disable virtual switch VLAN.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable virtual switch VLAN.		
	<i>disable</i>	Disable virtual switch VLAN.		
revision-image-auto-backup	Enable/disable back-up of the latest configuration revision after the firmware is upgraded.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable revision image backup automatically when upgrading image.		
	<i>disable</i>	Disable revision image backup automatically when upgrading image.		
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		
	<i>enable</i>	Enable revision config backup automatically when logout.		
	<i>disable</i>	Disable revision config backup automatically when logout.		
management-vdom	Management virtual domain name.	string	Maximum length: 31	root

Parameter	Description	Type	Size	Default						
hostname	FortiGate unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35							
alias	Alias for your FortiGate 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						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr> <tr> <td><i>disable</i></td><td>Disable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.	<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.			
Option	Description									
<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.									
<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.									
ssh-cbc-cipher	Enable/disable CBC cipher for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable CBC cipher for SSH access.</td></tr> <tr> <td><i>disable</i></td><td>Disable CBC cipher for SSH access.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable CBC cipher for SSH access.	<i>disable</i>	Disable CBC cipher for SSH access.			
Option	Description									
<i>enable</i>	Enable CBC cipher for SSH access.									
<i>disable</i>	Disable CBC cipher for SSH access.									
ssh-hmac-md5	Enable/disable HMAC-MD5 for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable HMAC-MD5 for SSH access.</td></tr> <tr> <td><i>disable</i></td><td>Disable HMAC-MD5 for SSH access.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HMAC-MD5 for SSH access.	<i>disable</i>	Disable HMAC-MD5 for SSH access.			
Option	Description									
<i>enable</i>	Enable HMAC-MD5 for SSH access.									
<i>disable</i>	Disable HMAC-MD5 for SSH access.									
ssh-kex-sha1	Enable/disable SHA1 key exchange for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable SHA1 for SSH key exchanges.</td></tr> <tr> <td><i>disable</i></td><td>Disable SHA1 for SSH key exchanges.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SHA1 for SSH key exchanges.	<i>disable</i>	Disable SHA1 for SSH key exchanges.			
Option	Description									
<i>enable</i>	Enable SHA1 for SSH key exchanges.									
<i>disable</i>	Disable SHA1 for SSH key exchanges.									
ssh-mac-weak	Enable/disable HMAC-SHA1 and UMAC-64-ETM for SSH access.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.</td></tr> <tr> <td><i>disable</i></td><td>Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.	<i>disable</i>	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.			
Option	Description									
<i>enable</i>	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.									
<i>disable</i>	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.									

Parameter	Description	Type	Size	Default																
ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-	enable																
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable static key ciphers in SSL/TLS connections.</td></tr> <tr> <td><i>disable</i></td><td>Disable static key ciphers in SSL/TLS connections.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable static key ciphers in SSL/TLS connections.	<i>disable</i>	Disable static key ciphers in SSL/TLS connections.													
Option	Description																			
<i>enable</i>	Enable static key ciphers in SSL/TLS connections.																			
<i>disable</i>	Disable static key ciphers in SSL/TLS connections.																			
snat-route-change	Enable/disable the ability to change the static NAT route.	option	-	disable																
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable SNAT route change.</td></tr> <tr> <td><i>disable</i></td><td>Disable SNAT route change.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SNAT route change.	<i>disable</i>	Disable SNAT route change.													
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																
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable speed test server service.</td></tr> <tr> <td><i>disable</i></td><td>Disable speed test server service.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable speed test server service.	<i>disable</i>	Disable speed test server service.													
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																
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable CLI audit log.</td></tr> <tr> <td><i>disable</i></td><td>Disable CLI audit log.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable CLI audit log.	<i>disable</i>	Disable CLI audit log.													
Option	Description																			
<i>enable</i>	Enable CLI audit log.																			
<i>disable</i>	Disable CLI audit log.																			
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048																
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>1024</i></td><td>1024 bits.</td></tr> <tr> <td><i>1536</i></td><td>1536 bits.</td></tr> <tr> <td><i>2048</i></td><td>2048 bits.</td></tr> <tr> <td><i>3072</i></td><td>3072 bits.</td></tr> <tr> <td><i>4096</i></td><td>4096 bits.</td></tr> <tr> <td><i>6144</i></td><td>6144 bits.</td></tr> <tr> <td><i>8192</i></td><td>8192 bits.</td></tr> </tbody> </table>	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.			
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.																			

Parameter	Description	Type	Size	Default
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
Option				
enable				
Enable FortiGuard statistics.				
disable				
Disable FortiGuard statistics.				
fds-statistics-period	FortiGuard statistics collection period in minutes. .	integer	Minimum value: 1 Maximum value: 1440	60
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable
Option				
enable				
Enable TCP option.				
disable				
Disable TCP option.				
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable
Option				
enable				
Enable transmission of Link Layer Discovery Protocol (LLDP).				
disable				
Disable transmission of Link Layer Discovery Protocol (LLDP).				
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable
Option				
enable				
Enable reception of Link Layer Discovery Protocol (LLDP).				
disable				
Disable reception of Link Layer Discovery Protocol (LLDP).				
proxy-auth-timeout	Authentication timeout in minutes for authenticated users .	integer	Minimum value: 1 Maximum value: 300	10

Parameter	Description	Type	Size	Default								
proxy-re-authentication-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 first created.	option	-	session								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>session</i></td><td>Proxy re-authentication timeout begins at the closure of the session.</td></tr> <tr> <td><i>traffic</i></td><td>Proxy re-authentication timeout begins after traffic has not been received.</td></tr> <tr> <td><i>absolute</i></td><td>Proxy re-authentication timeout begins when the user was first created.</td></tr> </tbody> </table>	Option	Description	<i>session</i>	Proxy re-authentication timeout begins at the closure of the session.	<i>traffic</i>	Proxy re-authentication timeout begins after traffic has not been received.	<i>absolute</i>	Proxy re-authentication timeout begins when the user was first created.			
Option	Description											
<i>session</i>	Proxy re-authentication timeout begins at the closure of the session.											
<i>traffic</i>	Proxy re-authentication timeout begins after traffic has not been received.											
<i>absolute</i>	Proxy re-authentication timeout begins when the user was first created.											
proxy-auth-lifetime	Enable/disable authenticated users lifetime control. This is a cap on the total time a proxy user can be authenticated for after which re-authentication will take place.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable authenticated users lifetime control.</td></tr> <tr> <td><i>disable</i></td><td>Disable authenticated users lifetime control.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable authenticated users lifetime control.	<i>disable</i>	Disable authenticated users lifetime control.					
Option	Description											
<i>enable</i>	Enable authenticated users lifetime control.											
<i>disable</i>	Disable authenticated users lifetime control.											
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users .	integer	Minimum value: 5 Maximum value: 65535	480								
proxy-resource-mode	Enable/disable use of the maximum memory usage on the FortiGate unit's proxy processing of resources, such as block lists, allow lists, and external resources.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
sys-perf-log-interval	Time in minutes between updates of performance statistics logging. .	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								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>loose</i>	Check protocol header loosely.		
	<i>strict</i>	Check protocol header strictly.		
vip-arp-range	Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.	option	-	restricted
	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.		
reset-sessionless-tcp	Action to perform if the FortiGate receives a TCP packet but cannot find a corresponding session in its session table. NAT/Route mode only.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reset session-less TCP.		
	<i>disable</i>	Disable reset session-less TCP.		
allow-traffic-redirect	Disable to prevent traffic with same local ingress and egress interface from being forwarded without policy check.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable allow traffic redirect.		
	<i>disable</i>	Disable allow traffic redirect.		
ipv6-allow-traffic-redirect	Disable to prevent IPv6 traffic with same local ingress and egress interface from being forwarded without policy check.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable allow traffic IPv6 redirect.		
	<i>disable</i>	Disable allow traffic IPv6 redirect.		

Parameter	Description	Type	Size	Default
strict-dirty-session-check	Enable to check the session against the original policy when revalidating. This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together. If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable strict dirty-session check.		
	<i>disable</i>	Disable strict dirty-session check.		
tcp-halfclose-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded .	integer	Minimum value: 1 Maximum value: 86400	120
tcp-halfopen-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded .	integer	Minimum value: 1 Maximum value: 86400	10
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds .	integer	Minimum value: 0 Maximum value: 300	1
tcp-rst-timer	Length of the TCP CLOSE state in seconds .	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 .	integer	Minimum value: 1 Maximum value: 86400	180
block-session-timer	Duration in seconds for blocked sessions .	integer	Minimum value: 1 Maximum value: 300	30
ip-src-port-range	IP source port range used for traffic originating from the FortiGate unit.	user	Not Specified	1024-25000

Parameter	Description	Type	Size	Default
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable pre-login banner.		
	<i>disable</i>	Disable pre-login banner.		
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable post-login banner.		
	<i>enable</i>	Enable post-login banner.		
tftp	Enable/disable TFTP.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TFTP.		
	<i>disable</i>	Disable TFTP.		
av-failopen	Set the action to take if the FortiGate is running low on memory or the proxy connection limit has been reached.	option	-	pass
	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.		

Parameter	Description	Type	Size	Default								
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme .	integer	Minimum value: 70 Maximum value: 97	95								
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode .	integer	Minimum value: 70 Maximum value: 97	88								
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode .	integer	Minimum value: 70 Maximum value: 97	82								
cpu-use-threshold	Threshold at which CPU usage is reported.	integer	Minimum value: 50 Maximum value: 99	90								
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
vdom-mode *	Enable/disable support for split/multiple virtual domains (VDOMs).	option	-	no-vdom								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>no-vdom</i></td><td>Disable split/multiple VDOMs mode.</td></tr> <tr> <td><i>split-vdom</i></td><td>Enable split VDOMs mode.</td></tr> <tr> <td><i>multi-vdom</i></td><td>Enable multiple VDOMs mode.</td></tr> </tbody> </table>					Option	Description	<i>no-vdom</i>	Disable split/multiple VDOMs mode.	<i>split-vdom</i>	Enable split VDOMs mode.	<i>multi-vdom</i>	Enable multiple VDOMs mode.
Option	Description											
<i>no-vdom</i>	Disable split/multiple VDOMs mode.											
<i>split-vdom</i>	Enable split VDOMs mode.											
<i>multi-vdom</i>	Enable multiple VDOMs mode.											
long-vdom-name *	Enable/disable long VDOM name support.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable long VDOM name support.</td></tr> <tr> <td><i>disable</i></td><td>Disable long VDOM name support.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable long VDOM name support.	<i>disable</i>	Disable long VDOM name support.		
Option	Description											
<i>enable</i>	Enable long VDOM name support.											
<i>disable</i>	Disable long VDOM name support.											
edit-vdom-prompt *	Enable/disable edit new VDOM prompt.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable edit new VDOM prompt.		
	<i>disable</i>	Disable edit new VDOM prompt.		
admin-port	Administrative access port for HTTP. .	integer	Minimum value: 1 Maximum value: 65535	80
admin-sport	Administrative access port for HTTPS. .	integer	Minimum value: 1 Maximum value: 65535	443
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-	enable
	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	15552000
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-	enable
	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.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local admin authentication restriction.		
	<i>disable</i>	Disable local admin authentication restriction.		

Parameter	Description	Type	Size	Default						
admin-ssh-port	Administrative access port for SSH. .	integer	Minimum value: 1 Maximum value: 65535	22						
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating .	integer	Minimum value: 10 Maximum value: 3600	120						
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable SSH v1 compatibility.</td></tr> <tr> <td><i>disable</i></td><td>Disable SSH v1 compatibility.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable SSH v1 compatibility.	<i>disable</i>	Disable SSH v1 compatibility.
Option	Description									
<i>enable</i>	Enable SSH v1 compatibility.									
<i>disable</i>	Disable SSH v1 compatibility.									
admin-telnet	Enable/disable TELNET service.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable TELNET service.</td></tr> <tr> <td><i>disable</i></td><td>Disable TELNET service.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable TELNET service.	<i>disable</i>	Disable TELNET service.
Option	Description									
<i>enable</i>	Enable TELNET service.									
<i>disable</i>	Disable TELNET service.									
admin-telnet-port	Administrative access port for TELNET. .	integer	Minimum value: 1 Maximum value: 65535	23						
admin-forticloud-sso-login	Enable/disable FortiCloud admin login via SSO.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable FortiCloud admin login via SSO.</td></tr> <tr> <td><i>disable</i></td><td>Disable FortiCloud admin login via SSO.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable FortiCloud admin login via SSO.	<i>disable</i>	Disable FortiCloud admin login via SSO.
Option	Description									
<i>enable</i>	Enable FortiCloud admin login via SSO.									
<i>disable</i>	Disable FortiCloud admin login via SSO.									
default-service-source-port	Default service source port range.	user	Not Specified							
admin-maintainer	Enable/disable maintainer administrator login. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password is "bcpb" followed by the FortiGate unit serial number. You have limited time to complete this login.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable login for special user (maintainer).		
	<i>disable</i>	Disable login for special user (maintainer).		
admin-reset-button *	press the reset button can reset to factory default	option	-	enable
	Option	Description		
	<i>enable</i>	press the reset button can reset to factory default		
	<i>disable</i>	press the reset button cannot reset to factory default		
admin-server-cert	Server certificate that the FortiGate uses for HTTPS administrative connections.	string	Maximum length: 35	self-sign
user-server-cert	Certificate to use for https user authentication.	string	Maximum length: 35	Fortinet_Factory
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		
	<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.		
	<i>disable</i>	Admin users can login by providing a valid certificate or password.		
wifi-certificate	Certificate to use for WiFi authentication.	string	Maximum length: 35	Fortinet_Wifi
wifi-ca-certificate	CA certificate that verifies the WiFi certificate.	string	Maximum length: 79	Fortinet_Wifi_CA
auth-http-port	User authentication HTTP port. .	integer	Minimum value: 1 Maximum value: 65535	1000
auth-https-port	User authentication HTTPS port. .	integer	Minimum value: 1 Maximum value: 65535	1003
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable use of keep alive to extend authentication.		
	<i>disable</i>	Disable use of keep alive to extend authentication.		
policy-auth-concurrent	Number of concurrent firewall user logins from the same user .	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
	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 FortiGate 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
	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 . 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
	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. .	integer	Minimum value: 10 Maximum value: 4294967295	600
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable
Option				
<i>enable</i>		Enable reboot of system upon restoring configuration.		
<i>disable</i>		Disable reboot of system upon restoring configuration.		
admin-scp	Enable/disable using SCP to download the system configuration. You can use SCP as an alternative method for backing up the configuration.	option	-	disable
Option				
<i>enable</i>		Enable allow system configuration download by SCP.		
<i>disable</i>		Disable allow system configuration download by SCP.		
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-	enable
Option				
<i>enable</i>		Enable submission of Security Rating results to FortiGuard.		
<i>disable</i>		Disable submission of Security Rating results to FortiGuard.		
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-	enable
Option				
<i>enable</i>		Enable scheduled runs of Security Rating.		
<i>disable</i>		Disable scheduled runs of Security Rating.		
wireless-controller	Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.	option	-	enable
Option				
<i>enable</i>		Enable wireless controller.		
<i>disable</i>		Disable wireless controller.		

Parameter	Description	Type	Size	Default						
wireless-controller-port	Port used for the control channel in wireless controller mode .	integer	Minimum value: 1024 Maximum value: 49150	5246						
fortiextender-data-port	FortiExtender data port .	integer	Minimum value: 1024 Maximum value: 49150	25246						
fortiextender	Enable/disable FortiExtender.	option	-	enable **						
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable FortiExtender controller.</td></tr> <tr> <td><i>enable</i></td><td>Enable FortiExtender controller.</td></tr> </tbody> </table>			Option	Description	<i>disable</i>	Disable FortiExtender controller.	<i>enable</i>	Enable FortiExtender controller.
Option	Description									
<i>disable</i>	Disable FortiExtender controller.									
<i>enable</i>	Enable FortiExtender controller.									
fortiextender-vlan-mode	Enable/disable FortiExtender VLAN mode.	option	-	disable						
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable FortiExtender VLAN mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable FortiExtender VLAN mode.</td></tr> </tbody> </table>			Option	Description	<i>enable</i>	Enable FortiExtender VLAN mode.	<i>disable</i>	Disable FortiExtender VLAN mode.
Option	Description									
<i>enable</i>	Enable FortiExtender VLAN mode.									
<i>disable</i>	Disable FortiExtender VLAN mode.									
switch-controller	Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself.	option	-	disable						
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable switch controller feature.</td></tr> <tr> <td><i>enable</i></td><td>Enable switch controller feature.</td></tr> </tbody> </table>			Option	Description	<i>disable</i>	Disable switch controller feature.	<i>enable</i>	Enable switch controller feature.
Option	Description									
<i>disable</i>	Disable switch controller feature.									
<i>enable</i>	Enable switch controller feature.									
switch-controller-reserved-network	Configure reserved network subnet for managed switches. This is available when the switch controller is enabled.	ipv4-classnet-host	Not Specified	10.255.0.0 255.255.0.0						
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: Maximum value: The number of logical CPUs.	1						

Parameter	Description	Type	Size	Default														
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1 **	1														
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 4 **	0														
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs.	integer	Minimum value: 2 Maximum value: 4 **	0														
proxy-hardware-acceleration *	Enable/disable email proxy hardware acceleration.	option	-	enable														
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable email proxy hardware acceleration.</td></tr> <tr> <td><i>enable</i></td><td>Enable email proxy hardware acceleration.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable email proxy hardware acceleration.	<i>enable</i>	Enable email proxy hardware acceleration.								
Option	Description																	
<i>disable</i>	Disable email proxy hardware acceleration.																	
<i>enable</i>	Enable email proxy hardware acceleration.																	
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-															
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.																	
ipsec-hmac-offload *	Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.	option	-	enable														
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable offload IPsec HMAC processing to hardware if possible.</td></tr> <tr> <td><i>disable</i></td><td>Disable offload IPsec HMAC processing to hardware.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.	<i>disable</i>	Disable offload IPsec HMAC processing to hardware.								
Option	Description																	
<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.																	
<i>disable</i>	Disable offload IPsec HMAC processing to hardware.																	

Parameter	Description	Type	Size	Default
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2	1
ipv6-allow-anycast-probe	Enable/disable IPv6 address probe through Anycast.	option	-	disable
Option		Description		
		<i>enable</i> Enable probing of IPv6 address space through Anycast		
		<i>disable</i> Disable probing of IPv6 address space through Anycast		
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable
Option		Description		
		<i>enable</i> Enable CA attribute in CSR.		
		<i>disable</i> Disable CA attribute in CSR.		
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable
Option		Description		
		<i>enable</i> Enable WiMax 4G.		
		<i>disable</i> Disable WiMax 4G.		
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8
sslvpn-max-worker-count	Maximum number of SSL-VPN processes. Upper limit for this value is the number of CPUs and depends on the model. Default value of zero means the SSLVPN daemon decides the number of worker processes.	integer	Minimum value: 0 Maximum value: 4 **	0
sslvpn-kxp-hardware-acceleration *	Enable/disable SSL-VPN KXP hardware acceleration.	option	-	enable **
Option		Description		
		<i>enable</i> Enable KXP SSL-VPN hardware acceleration.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.		
sslvpn-cipher-hardware-acceleration *	Enable/disable SSL-VPN hardware acceleration.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.		
	<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.		
sslvpn-ems-sn-check	Enable/disable verification of EMS serial number in SSL-VPN connection.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable verification of EMS serial number in SSL-VPN connection.		
	<i>disable</i>	Disable verification of EMS serial number in SSL-VPN connection.		
sslvpn-plugin-version-check	Enable/disable checking browser's plugin version by SSL-VPN.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.		
	<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.		
two-factor-ftk-expiry	FortiToken authentication session timeout .	integer	Minimum value: 60 Maximum value: 600	60
two-factor-email-expiry	Email-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300	60
two-factor-sms-expiry	SMS-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300	60
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout .	integer	Minimum value: 10 Maximum value: 3600	60

Parameter	Description	Type	Size	Default
two-factor-ftm-expiry	FortiToken Mobile session timeout .	integer	Minimum value: 1 Maximum value: 168	72
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: 4 **	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: 4 **	0
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-	enable
Option	Description			
disable	Disable dispatching traffic to WAD workers based on source affinity.			
enable	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			
enable	Enable login time recording.			
disable	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. No logs will be dropped or lost if the number is changed.	integer	Minimum value: 0 Maximum value: 15	0

Parameter	Description	Type	Size	Default						
special-file-23-support	Enable/disable detection of those special format files when using Data Leak Protection.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable detection of those special format files when using Data Leak Protection.</td></tr> <tr> <td><i>enable</i></td><td>Enable detection of those special format files when using Data Leak Protection.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable detection of those special format files when using Data Leak Protection.	<i>enable</i>	Enable detection of those special format files when using Data Leak Protection.			
Option	Description									
<i>disable</i>	Disable detection of those special format files when using Data Leak Protection.									
<i>enable</i>	Enable detection of those special format files when using Data Leak Protection.									
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable insertion of address UUID to traffic logs.</td></tr> <tr> <td><i>disable</i></td><td>Disable insertion of address UUID to traffic logs.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable insertion of address UUID to traffic logs.	<i>disable</i>	Disable insertion of address UUID to traffic logs.			
Option	Description									
<i>enable</i>	Enable insertion of address UUID to traffic logs.									
<i>disable</i>	Disable insertion of address UUID to traffic logs.									
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable logging of SSL connection events.</td></tr> <tr> <td><i>disable</i></td><td>Disable logging of SSL connection events.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable logging of SSL connection events.	<i>disable</i>	Disable logging of SSL connection events.			
Option	Description									
<i>enable</i>	Enable logging of SSL connection events.									
<i>disable</i>	Disable logging of SSL connection events.									
gui-rest-api-cache	Enable/disable REST API result caching on FortiGate.	option	-	enable **						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable REST API result caching on FortiGate.</td></tr> <tr> <td><i>disable</i></td><td>Disable REST API result caching on FortiGate.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable REST API result caching on FortiGate.	<i>disable</i>	Disable REST API result caching on FortiGate.			
Option	Description									
<i>enable</i>	Enable REST API result caching on FortiGate.									
<i>disable</i>	Disable REST API result caching on FortiGate.									
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table .	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 xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0						
cmdbsvr-affinity	Affinity setting for cmdbsvr (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0						

Parameter	Description	Type	Size	Default						
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	integer	Minimum value: 0 Maximum value: 2147483647	0						
ipsec-asic-offload *	Enable/disable ASIC offloading (hardware acceleration) for IPsec VPN traffic. Hardware acceleration can offload IPsec VPN sessions and accelerate encryption and decryption.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable ASIC offload for IPsec VPN.</td></tr> <tr> <td><i>disable</i></td><td>Disable ASIC offload for IPsec VPN.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable ASIC offload for IPsec VPN.	<i>disable</i>	Disable ASIC offload for IPsec VPN.
Option	Description									
<i>enable</i>	Enable ASIC offload for IPsec VPN.									
<i>disable</i>	Disable ASIC offload for IPsec VPN.									
ipsec-soft-dec-async	Enable/disable software decryption synchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable software decryption synchronization for IPsec VPN.</td></tr> <tr> <td><i>disable</i></td><td>Disable software decryption synchronization for IPsec VPN.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable software decryption synchronization for IPsec VPN.	<i>disable</i>	Disable software decryption synchronization for IPsec VPN.
Option	Description									
<i>enable</i>	Enable software decryption synchronization for IPsec VPN.									
<i>disable</i>	Disable software decryption synchronization for IPsec VPN.									
device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out. .	integer	Minimum value: 30 Maximum value: 31536000	300						

Parameter	Description	Type	Size	Default												
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 15934 Maximum value: 45528 **	31869 **												
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 15934 Maximum value: 45528 **	31869 **												
gui-device-latitude	Add the latitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19													
gui-device-longitude	Add the longitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19													
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-	disable												
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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												
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.
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.															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>retro</i>	FortiOS v3 Retro theme.		
	<i>dark-matter</i>	Dark Matter theme.		
	<i>onyx</i>	Onyx theme.		
	<i>eclipse</i>	Eclipse theme.		
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd
	Option	Description		
	<i>yyyy/MM/dd</i>	Year/Month/Day.		
	<i>dd/MM/yyyy</i>	Day/Month/Year.		
	<i>MM/dd/yyyy</i>	Month/Day/Year.		
	<i>yyyy-MM-dd</i>	Year-Month-Day.		
	<i>dd-MM-yyyy</i>	Day-Month-Year.		
	<i>MM-dd-yyyy</i>	Month-Day-Year.		
gui-date-time-source	Source from which the FortiGate GUI uses to display date and time entries.	option	-	system
	Option	Description		
	<i>system</i>	Use this FortiGate unit's configured timezone.		
	<i>browser</i>	Use the web browser's timezone.		
igmp-state-limit	Maximum number of IGMP memberships .	integer	Minimum value: 96 Maximum value: 128000	3200
legacy-poe-device-support *	Enable/disable legacy POE device support.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable legacy POE device support.		
	<i>disable</i>	Disable legacy POE device support.		
cloud-communication	Enable/disable all cloud communication.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Allow cloud communication.		
	disable	Disable all cloud-related settings.		
		 When set to <i>disable</i> , cloud-related settings (for example, config system autoupdate tunneling on page 1051 status) will be disabled. When a user issues the command to change one of these settings, it will fail with the message <i>cloud communication is disabled in 'system.global'</i> .		
fec-port	Local UDP port for Forward Error Correction .	integer	Minimum value: 49152 Maximum value: 65535	50000
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		
	enable	Enable FortiToken Cloud service.		
	disable	Disable FortiToken Cloud service.		
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	Minimum value: 0 Maximum value: 214748364	0
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto
	Option	Description		
	auto	Automatically switch CPU accounting mode.		
	force	Force the use of CPU IRQ time accounting mode.		
fortiipam-integration	Enable/disable integration with the FortiIPAM cloud service.	option	-	enable
	Option	Description		
	enable	Enable integration with FortiIPAM for automatic IP address management.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<code>disable</code>	Disable integration with FortiIPAM for automatic IP address management.			
management-ip	Management IP address of this FortiGate. Used to log into this FortiGate from another FortiGate in the Security Fabric.	string	Maximum length: 255		
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 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			
	<code>enable</code>	Enable use of the admin-sport setting for the management port.			
	<code>disable</code>	Disable use of the admin-sport setting for the management port.			

* This parameter may not exist in some models.

** Values may differ between models.

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 wifi [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 data-loss-prevention [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|...]
end
set admintimeout-override [enable|disable]
set admintimeout {integer}
set system-diagnostics [enable|disable]
next
end

```

config system accprofile

Parameter	Description	Type	Size	Default
scope	Scope of admin access: global or specific VDOM(s).	option	-	vdom
Parameter	Description	Type	Size	Default
Option	Description			
<i>vdom</i>	VDOM access.			
<i>global</i>	Global access.			

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
secfabgrp	Security Fabric.	option	-	none
		Option	Description	
		<i>none</i>	No access.	
		<i>read</i>	Read access.	
		<i>read-write</i>	Read/write access.	
ftviewgrp	FortiView.	option	-	none
		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
		Option	Description	
		<i>none</i>	No access.	
		<i>read</i>	Read access.	
		<i>read-write</i>	Read/write access.	
sysgrp	System Configuration.	option	-	none
		Option	Description	
		<i>none</i>	No access.	
		<i>read</i>	Read access.	
		<i>read-write</i>	Read/write access.	
		<i>custom</i>	Customized access.	
netgrp	Network Configuration.	option	-	none
		Option	Description	
		<i>none</i>	No access.	
		<i>read</i>	Read access.	
		<i>read-write</i>	Read/write access.	
		<i>custom</i>	Customized access.	

Parameter	Description	Type	Size	Default
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
fwgrp	Administrator access to the Firewall configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-	none
	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
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
wifi	Administrator access to the WiFi controller and Switch controller.	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.		
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable
	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 .	integer	Minimum value: 1 Maximum value: 480	10
system-diagnostics	Enable/disable permission to run system diagnostic commands.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable permission to run system diagnostic commands.		
	<i>disable</i>	Disable permission to run system diagnostic commands.		

config netgrp-permission

Parameter	Description	Type	Size	Default
cfg	Network Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
packet-capture	Packet Capture Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

Parameter	Description	Type	Size	Default
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
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
	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
	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.		

Parameter	Description	Type	Size	Default								
ips	IPS profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
webfilter	Web Filter profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
emailfilter	Email Filter and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
data-loss-prevention	DLP profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
file-filter	File-filter profiles and settings.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
application-control	Application Control 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.		
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.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config system npu



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61F. It is not available for FortiGate VM64.

Configure NPU attributes.

```
config system npu
  Description: Configure NPU attributes.
  set iph-rsvd-re-cksum [enable|disable]
  set per-session-accounting [disable|traffic-log-only|...]
  config fp-anomaly
    Description: NP6Lite anomaly protection (packet drop or send trap to host).
    set ipv4-ver-err [drop|trap-to-host]
    set ipv4-ihl-err [drop|trap-to-host]
    set ipv4-len-err [drop|trap-to-host]
    set ipv4-ttlzero-err [drop|trap-to-host]
    set ipv4-csum-err [drop|trap-to-host]
    set ipv4-opt-err [drop|trap-to-host]
    set tcp-hlen-err [drop|trap-to-host]
    set tcp-plen-err [drop|trap-to-host]
    set tcp-csum-err [drop|trap-to-host]
    set udp-plen-err [drop|trap-to-host]
    set udp-hlen-err [drop|trap-to-host]
    set udp-csum-err [drop|trap-to-host]
    set udp-len-err [drop|trap-to-host]
    set udplite-cover-err [drop|trap-to-host]
    set udplite-csum-err [drop|trap-to-host]
    set icmp-minlen-err [drop|trap-to-host]
    set icmp-csum-err [drop|trap-to-host]
    set esp-minlen-err [drop|trap-to-host]
    set unknproto-minlen-err [drop|trap-to-host]
    set ipv6-ver-err [drop|trap-to-host]
    set ipv6-ihl-err [drop|trap-to-host]
    set ipv6-plen-zero [drop|trap-to-host]
    set ipv6-exthdr-order-err [drop|trap-to-host]
    set ipv6-exthdr-len-err [drop|trap-to-host]
  end
end
```

config system npu

Parameter	Description	Type	Size	Default
iph-rsvd-recksum *	Enable/disable IP checksum re-calculation for packets with iph.reserved bit set.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IP checksum re-calculation for packets with iph.reserved bit set.		
	<i>disable</i>	Disable IP checksum re-calculation for packets with iph.reserved bit set.		
per-session-accounting *	Enable/disable per-session accounting.	option	-	traffic-log-only
	Option	Description		
	<i>disable</i>	Disable per-session accounting.		
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.		
	<i>enable</i>	Per-session accounting for all sessions.		

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size	Default
ipv4-ver-err	Invalid IPv4 header version anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid header version.		
	<i>trap-to-host</i>	Forward IPv4 invalid header version to main CPU for processing.		
ipv4-ihl-err	Invalid IPv4 header length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid header length.		
	<i>trap-to-host</i>	Forward IPv4 invalid header length to main CPU for processing.		
ipv4-len-err	Invalid IPv4 packet length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid packet length to main CPU for processing.		

Parameter	Description	Type	Size	Default
ipv4-ttlzero-err	Invalid IPv4 TTL field zero anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid TTL field zero.		
	<i>trap-to-host</i>	Forward IPv4 invalid TTL field zero to main CPU for processing.		
ipv4-csum-err	Invalid IPv4 packet checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid L3 checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid L3 checksum to main CPU for processing.		
ipv4-opt-err	Invalid IPv4 option parsing anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid option parsing.		
	<i>trap-to-host</i>	Forward IPv4 invalid option parsing to main CPU for processing.		
tcp-hlen-err	Invalid IPv4 TCP header length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid TCP packet header length.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet header length to main CPU for processing.		
tcp-plen-err	Invalid IPv4 TCP packet length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid TCP packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet length to main CPU for processing.		
tcp-csum-err	Invalid IPv4 TCP packet checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid TCP packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet checksum to main CPU for processing.		
udp-plen-err	Invalid IPv4 UDP packet minimum length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP packet minimum length.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet minimum length to main CPU for processing.		
udp-hlen-err	Invalid IPv4 UDP packet header length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP header length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP header length to main CPU for processing.		
udp-csum-err	Invalid IPv4 UDP packet checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet checksum to main CPU for processing.		
udp-len-err	Invalid IPv4 UDP packet length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet length to main CPU for processing.		
udplite-cover-err	Invalid IPv4 UDP-Lite packet coverage anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP-Lite packet coverage.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.		
udplite-csum-err	Invalid IPv4 UDP-Lite packet checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid UDP-Lite packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.		
icmp-minlen-err	Invalid IPv4 ICMP short packet anomalies.	option	-	drop

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid ICMP short packet.		
	<i>trap-to-host</i>	Forward IPv4 invalid ICMP short packet to main CPU for processing.		
icmp-csum-err	Invalid IPv4 ICMP packet checksum anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid ICMP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.		
esp-minlen-err	Invalid IPv4 ESP short packet anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid ESP short packet.		
	<i>trap-to-host</i>	Forward IPv4 invalid ESP short packet to main CPU for processing.		
unknproto-minlen-err	Invalid IPv4 L4 unknown protocol short packet anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv4 invalid L4 unknown protocol short packet.		
	<i>trap-to-host</i>	Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.		
ipv6-ver-err	Invalid IPv6 packet version anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv6 with invalid packet version.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet version to FortiOS.		
ipv6-ihl-err	Invalid IPv6 packet length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv6 with invalid packet length.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet length to FortiOS.		
ipv6-plen-zero	Invalid IPv6 packet payload length zero anomalies.	option	-	drop

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>drop</i>	Drop IPv6 with invalid packet payload length zero.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet payload length zero to FortiOS.		
ipv6-exthdr-order-err	Invalid IPv6 packet extension header ordering anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv6 with invalid packet extension header ordering.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet extension header ordering to FortiOS.		
ipv6-exthdr-len-err	Invalid IPv6 packet chain extension header total length anomalies.	option	-	drop
	Option	Description		
	<i>drop</i>	Drop IPv6 with invalid packet chain extension header total length.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet chain extension header total length to FortiOS.		

config system vdom-link

Configure VDOM links.

```
config system vdom-link
  Description: Configure VDOM links.
  edit <name>
    set vcluster [vcluster1|vcluster2]
    set type [ppp|ethernet]
  next
end
```

config system vdom-link

Parameter	Description	Type	Size	Default
vcluster	Virtual cluster.	option	-	vcluster1
	Option	Description		
	<i>vcluster1</i>	Virtual cluster 1.		
	<i>vcluster2</i>	Virtual cluster 2.		
type	VDOM link type: PPP or Ethernet.	option	-	ppp

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ppp</i>	PPP VDOM link.		
	<i>ethernet</i>	Ethernet VDOM link.		

config system switch-interface

Configure software switch interfaces by grouping physical and WiFi interfaces.

```
config system switch-interface
  Description: Configure software switch interfaces by grouping physical and WiFi interfaces.
  edit <name>
    set vdom {string}
    set span-dest-port {string}
    set span-source-port <interface-name1>, <interface-name2>, ...
    set member <interface-name1>, <interface-name2>, ...
    set type [switch|hub]
    set intra-switch-policy [implicit|explicit]
    set mac-ttl {integer}
    set span [disable|enable]
    set span-direction [rx|tx|...]
  next
end
```

config system switch-interface

Parameter	Description	Type	Size	Default
vdom	VDOM that the software switch belongs to.	string	Maximum length: 31	
span-dest-port	SPAN destination port name. All traffic on the SPAN source ports is echoed to the SPAN destination port.	string	Maximum length: 15	
span-source-port <interface-name>	Physical interface name. Port spanning echoes all traffic on the SPAN source ports to the SPAN destination port. Physical interface name.	string	Maximum length: 79	
member <interface-name>	Names of the interfaces that belong to the virtual switch. Physical interface name.	string	Maximum length: 79	
type	Type of switch based on functionality: switch for normal functionality, or hub to duplicate packets to all port members.	option	-	switch

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>switch</i>	Switch for normal switch functionality (available in NAT mode only).		
	<i>hub</i>	Hub to duplicate packets to all member ports.		
intra-switch-policy	Allow any traffic between switch interfaces or require firewall policies to allow traffic between switch interfaces.	option	-	implicit
	Option	Description		
	<i>implicit</i>	Traffic between switch members is implicitly allowed.		
	<i>explicit</i>	Traffic between switch members must match firewall policies.		
mac-ttl	Duration for which MAC addresses are held in the ARP table .	integer	Minimum value: 300 Maximum value: 8640000	300
span	Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span destination port.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable port spanning.		
	<i>enable</i>	Enable port spanning.		
span-direction	The direction in which the SPAN port operates, either: rx, tx, or both.	option	-	both
	Option	Description		
	<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.		
	<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.		
	<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.		

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								
address	Address.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>mandatory</i></td><td>Mandatory.</td></tr> <tr> <td><i>optional</i></td><td>Optional.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>mandatory</i>	Mandatory.	<i>optional</i>	Optional.			
Option	Description											
<i>disable</i>	Disable.											
<i>mandatory</i>	Mandatory.											
<i>optional</i>	Optional.											
device	Device.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>mandatory</i></td><td>Mandatory.</td></tr> <tr> <td><i>optional</i></td><td>Optional.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>mandatory</i>	Mandatory.	<i>optional</i>	Optional.			
Option	Description											
<i>disable</i>	Disable.											
<i>mandatory</i>	Mandatory.											
<i>optional</i>	Optional.											
interface	Interface.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>mandatory</i></td><td>Mandatory.</td></tr> <tr> <td><i>optional</i></td><td>Optional.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>mandatory</i>	Mandatory.	<i>optional</i>	Optional.			
Option	Description											
<i>disable</i>	Disable.											
<i>mandatory</i>	Mandatory.											
<i>optional</i>	Optional.											
multiple	Allow multiple tag selection.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable multi-tagging.</td></tr> <tr> <td><i>disable</i></td><td>Disable multi-tagging.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable multi-tagging.	<i>disable</i>	Disable multi-tagging.					
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								

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

config system lte-modem



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61F. It is not available for FortiGate VM64.

Configure USB LTE/WIMAX devices.

```
config system lte-modem
  Description: Configure USB LTE/WIMAX devices.
  set status [enable|disable]
  set extra-init {string}
  set authtype [none|pap|...]
  set username {string}
  set passwd {password}
  set apn {string}
  set modem-port {integer}
  set mode [standalone|redundant]
  set holddown-timer {integer}
  set interface {string}
end
```

config system lte-modem

Parameter	Description	Type	Size	Default
status	Enable/disable USB LTE/WIMAX device.	option	-	disable
Option		Description		
<i>enable</i>		Enable USB LTE/WIMA device.		
<i>disable</i>		Disable USB LTE/WIMA device.		
extra-init	Extra initialization string for USB LTE/WIMAX devices.	string	Maximum length: 127	
authtype	Authentication type for PDP-IP packet data calls.	option	-	none
Option		Description		
<i>none</i>		Username and password not required.		
<i>pap</i>		Use PAP authentication.		
<i>chap</i>		Use CHAP authentication.		

Parameter	Description	Type	Size	Default
username	Authentication username for PDP-IP packet data calls.	string	Maximum length: 63	
passwd	Authentication password for PDP-IP packet data calls.	password	Not Specified	
apn	Login APN string for PDP-IP packet data calls.	string	Maximum length: 127	
modem-port	Modem port index .	integer	Minimum value: 0 Maximum value: 20	255
mode	Modem operation mode.	option	-	standalone
Option	Description			
<i>standalone</i>	Standalone modem operation mode.			
<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.			
holddown-timer	Hold down timer .	integer	Minimum value: 10 Maximum value: 60	30
interface	The interface that the modem is acting as a redundant interface for.	string	Maximum length: 63	

config system interface

Configure interfaces.

```
config system interface
  Description: Configure interfaces.
  edit <name>
    set vdom {string}
    set vrf {integer}
    set cli-conn-status {integer}
    set fortilink [enable|disable]
    set switch-controller-source-ip [outbound|fixed]
    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|sdwan|...]
set dhcp-relay-interface {string}
set dhcp-relay-service [disable|enable]
set dhcp-relay-ip {user}
set dhcp-relay-request-all-server [disable|enable]
set dhcp-relay-type [regular|ipsec]
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-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 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 ndiscforward [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 vlanforward [enable|disable]
```

```
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set ips-sniffer-mode [enable|disable]
set ident-accept [enable|disable]
set ipmac [enable|disable]
set subst [enable|disable]
set macaddr {mac-address}
set substitute-dst-mac {mac-address}
set poe [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 mtu-override [enable|disable]
set mtu {integer}
set wccp [enable|disable]
set netflow-sampler [disable|tx|...]
set sflow-sampler [enable|disable]
set drop-overlapped-fragment [enable|disable]
set drop-fragment [enable|disable]
set src-check [enable|disable]
set sample-rate {integer}
set polling-interval {integer}
set sample-direction [tx|rx|...]
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 disconnect-threshold {integer}
set spillover-threshold {integer}
set ingress-spillover-threshold {integer}
set weight {integer}
set interface {string}
set external [enable|disable]
set vlan-protocol [8021q|8021ad]
set vlanid {integer}
set trunk [enable|disable]
set forward-domain {integer}
set remote-ip {ipv4-classnet-host}
set member <interface-name1>, <interface-name2>, ...
set lacp-mode [static|passive|...]
set lacp-ha-slave [enable|disable]
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 priority-override {enable|disable}
set aggregate {string}
set redundant-interface {string}
set devindex {integer}
set vindex {integer}
set switch {string}
set description {var-string}
set alias {string}
set l2tp-client [enable|disable]
config l2tp-client-settings
    Description: L2TP client settings.
    set user {string}
    set password {password}
    set peer-host {string}
    set peer-mask {ipv4-netmask}
    set peer-port {integer}
    set auth-type [auto|pap|...]
    set mtu {integer}
    set distance {integer}
    set priority {integer}
    set defaultgw [enable|disable]
    set ip {ipv4-classnet-host}
end
set security-mode [none|captive-portal|...]
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-8021x-mode [default|dynamic-vlan|...]
set security-8021x-master {string}
set security-8021x-dynamic-vlan-id {integer}
set security-external-web {var-string}
set security-external-logout {string}
set replacemsg-override-group {string}
set security-redirect-url {var-string}
set security-exempt-list {string}
set security-groups <name1>, <name2>, ...
set stp [disable|enable]
set stp-ha-secondary [disable|enable|...]
set device-identification [enable|disable]
set device-user-identification [enable|disable]
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set lldp-network-policy {string}
set estimated-upstream-bandwidth {integer}
set estimated-downstream-bandwidth {integer}
set measured-upstream-bandwidth {integer}
set measured-downstream-bandwidth {integer}
set bandwidth-measure-time {integer}
set monitor-bandwidth [enable|disable]
set vrrp-virtual-mac [enable|disable]
config vrrp
    Description: VRRP configuration.
    edit <vrnid>
        set version [2|3]
        set vrgrp {integer}
        set vrip {ipv4-address-any}
        set priority {integer}

```

```

        set adv-interval {integer}
        set start-time {integer}
        set preempt [enable|disable]
        set accept-mode [enable|disable]
        set vrdst {ipv4-address-any}
        set vrdst-priority {integer}
        set ignore-default-route [enable|disable]
        set status [enable|disable]
        config proxy-arp
            Description: VRRP Proxy ARP configuration.
            edit <id>
                set ip {user}
            next
        end
    next
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 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 preserve-session-route [enable|disable]
set auto-auth-extension-device [enable|disable]
set ap-discover [enable|disable]
set fortilink-neighbor-detect [lldp|fortilink]
set ip-managed-by-fortiipam [enable|disable]
set managed-subnetwork-size [256|512|...]
set fortilink-split-interface [enable|disable]
set internal {integer}
set fortilink-backup-link {integer}
set switch-controller-access-vlan [enable|disable]
set switch-controller-traffic-policy {string}
set switch-controller-rspan-mode [disable|enable]
set switch-controller-mgmt-vlan {integer}
set switch-controller-igmp-snooping [enable|disable]
set switch-controller-igmp-snooping-proxy [enable|disable]
set switch-controller-igmp-snooping-fast-leave [enable|disable]
set switch-controller-dhcp-snooping [enable|disable]
set switch-controller-dhcp-snooping-verify-mac [enable|disable]
set switch-controller-dhcp-snooping-option82 [enable|disable]
config dhcp-snooping-server-list
    Description: Configure DHCP server access list.
    edit <name>
        set server-ip {ipv4-address}
    next
end
set switch-controller-arp-inspection [enable|disable]

```

```

set switch-controller-learning-limit {integer}
set switch-controller-nac {string}
set switch-controller-dynamic {string}
set switch-controller-feature [none|default-vlan|...]
set switch-controller-iot-scanning [enable|disable]
set swc-vlan {integer}
set swc-first-create {integer}
set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
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-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 rdnss {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 autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set subnet {ipv6-network}
        set rdnss-service [delegated|default|...]
        set rdnss {user}
    next
end
set dhcp6-relay-service [disable|enable]
set dhcp6-relay-type {option}
set dhcp6-relay-ip {user}
set dhcp6-client-options {option1}, {option2}, ...
set dhcp6-prefix-delegation [enable|disable]
set dhcp6-information-request [enable|disable]
set dhcp6-prefix-hint {ipv6-network}
set dhcp6-prefix-hint-plt {integer}
set dhcp6-prefix-hint-vlt {integer}
set cli-conn6-status {integer}
set vrrp-virtual-mac6 [enable|disable]
set vrip6_link_local {ipv6-address}
config vrrp6
    Description: IPv6 VRRP configuration.
    edit <vrnid>
        set vrgrp {integer}
        set vrip6 {ipv6-address}
        set priority {integer}
        set adv-interval {integer}
        set start-time {integer}
        set preempt [enable|disable]
        set accept-mode [enable|disable]
        set vrdst6 {ipv6-address}
        set status [enable|disable]
    next
end
end
next
end

```

config system interface

Parameter	Description	Type	Size	Default
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0
fortilink	Enable FortiLink to dedicate this interface to manage other Fortinet devices.	option	-	disable
Option		Description		
		<i>enable</i> Enable FortiLink to dedicated interface for managing FortiSwitch devices.		
		<i>disable</i> Disable FortiLink to dedicated interface for managing FortiSwitch devices.		
switch-controller-source-ip	Source IP address used in FortiLink over L3 connections.	option	-	outbound
Option		Description		
		<i>outbound</i> Source IP address is that of the outbound interface.		
		<i>fixed</i> Source IP address is that of the FortiLink interface.		
mode	Addressing mode (static, DHCP, PPPoE).	option	-	static
Option		Description		
		<i>static</i> Static setting.		
		<i>dhcp</i> External DHCP client mode.		
		<i>pppoe</i> External PPPoE mode.		
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: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
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-request-all-server	Enable/disable sending of DHCP requests to all servers.	option	-	disable
	Option	Description		
	<i>disable</i>	Send DHCP requests only to a matching server.		
	<i>enable</i>	Send DHCP requests to all servers.		
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular
	Option	Description		
	<i>regular</i>	Regular DHCP relay.		
	<i>ipsec</i>	DHCP relay for IPsec.		
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DHCP relay agent option.		
	<i>disable</i>	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	-	disable **
	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	-	
	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
	Option	Description		
	<i>enable</i>	Enable detect gateway alive for first.		
	<i>disable</i>	Disable detect gateway alive for first.		

Parameter	Description	Type	Size	Default
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
fail-detect	Enable/disable fail detection features for this interface.	option	-	disable
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
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
Option		Description		
		<i>link-failed-signal</i>	Link-failed-signal.	
		<i>link-down</i>	Link-down.	
fail-action-on-extender	Action on extender when interface fail .	option	-	soft-restart

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>soft-restart</i>	Soft-restart-on-extender.		
	<i>hard-restart</i>	Hard-restart-on-extender.		
	<i>reboot</i>	Reboot-on-extender.		
fail-alert-interfaces <name>	Names of the FortiGate interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 79	
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48	
dhcp-renew-time	DHCP renew time in seconds , 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-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable
	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 .	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
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							
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable default gateway.</td></tr> <tr> <td>disable</td><td>Disable default gateway.</td></tr> </tbody> </table>					Option	Description	enable	Enable default gateway.	disable	Disable default gateway.
Option	Description									
enable	Enable default gateway.									
disable	Disable default gateway.									
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Use DNS acquired by DHCP or PPPoE.</td></tr> <tr> <td>disable</td><td>No not use DNS acquired by DHCP or PPPoE.</td></tr> </tbody> </table>					Option	Description	enable	Use DNS acquired by DHCP or PPPoE.	disable	No not use DNS acquired by DHCP or PPPoE.
Option	Description									
enable	Use DNS acquired by DHCP or PPPoE.									
disable	No not use DNS acquired by DHCP or PPPoE.									
auth-type	PPP authentication type to use.	option	-	auto						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>auto</td><td>Automatically choose authentication.</td></tr> </tbody> </table>					Option	Description	auto	Automatically choose authentication.		
Option	Description									
auto	Automatically choose authentication.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
<code>pptp-client</code>	Enable/disable PPTP client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PPTP client.		
	<i>disable</i>	Disable PPTP client.		
<code>pptp-user</code>	PPTP user name.	string	Maximum length: 64	
<code>pptp-password</code>	PPTP password.	password	Not Specified	
<code>pptp-server-ip</code>	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0
<code>pptp-auth-type</code>	PPTP authentication type.	option	-	auto
	Option	Description		
	<i>auto</i>	Automatically choose authentication.		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
<code>pptp-timeout</code>	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0
<code>arpforward</code>	Enable/disable ARP forwarding.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ARP forwarding.		
	<i>disable</i>	Disable ARP forwarding.		
<code>ndiscforward</code>	Enable/disable NDISC forwarding.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable NDISC forwarding.		
	<i>disable</i>	Disable NDISC forwarding.		
broadcast-forward	Enable/disable broadcast forwarding.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable broadcast forwarding.		
	<i>disable</i>	Disable broadcast forwarding.		
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-	global
	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
	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sending of ICMP redirects.		
	<i>disable</i>	Disable sending of ICMP redirects.		
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ICMP accept redirect.		
	<i>disable</i>	Disable ICMP accept redirect.		
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable traffic forwarding.		
	<i>disable</i>	Disable traffic forwarding.		
stpforward	Enable/disable STP forwarding.	option	-	disable
	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
	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.		
ips-sniffer-mode	Enable/disable the use of this interface as a one-armed sniffer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPS sniffer mode.		
	<i>disable</i>	Disable IPS sniffer mode.		
ident-accept	Enable/disable authentication for this interface.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable determining a user's identity from packet identification.		
	<i>disable</i>	Disable determining a user's identity from packet identification.		
ipmac	Enable/disable IP/MAC binding.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IP/MAC binding.		
	<i>disable</i>	Disable IP/MAC binding.		
subst	Enable to always send packets from this interface to a destination MAC address.	option	-	disable
	Option	Description		
	<i>enable</i>	Send packets from this interface.		
	<i>disable</i>	Do not send packets from this interface.		
macaddr	Change the interface's MAC address.	mac-address	Not Specified	**
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
poe *	Enable/disable PoE status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable PoE status.		
	<i>disable</i>	Disable PoE status.		
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-	auto
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>1000full</i>	1000M full-duplex.		
	<i>1000half</i>	1000M half-duplex.		
	<i>1000auto</i>	1000M auto adjust.		
status	Bring the interface up or shut the interface down.	option	-	up
	Option	Description		
	<i>up</i>	Bring the interface up.		
	<i>down</i>	Shut the interface down.		
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable
	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
type	Interface type.	option	-	vlan
	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>vdom-link</i>	VDOM link interface.		
	<i>loopback</i>	Loopback interface.		
	<i>switch</i>	Software switch interface.		
	<i>hard-switch</i>	Hardware switch interface.		
	<i>vap-switch</i>	VAP interface.		
	<i>wl-mesh</i>	WLAN mesh interface.		
	<i>fext-wan</i>	FortiExtender interface.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>vxlan</i>	VXLAN interface.		
	<i>geneve</i>	GENEVE interface.		
	<i>hdlc</i>	T1/E1 interface.		
	<i>switch-vlan</i>	Switch VLAN interface.		
	<i>emac-vlan</i>	EMAC VLAN interface.		
	<i>ssl</i>	SSL-VPN client interface.		
dedicated-to	Configure interface for single purpose.	option	-	none
	Option	Description		
	<i>none</i>	Interface not dedicated for any purpose.		
	<i>management</i>	Dedicate this interface for management purposes only.		
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
mtu-override	Enable to set a custom MTU for this interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Override default MTU.		
	<i>disable</i>	Use default MTU.		

Parameter	Description	Type	Size	Default										
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500										
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.													
netflow-sampler	Enable/disable NetFlow on this interface and set the data that NetFlow collects (rx, tx, or both).	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable NetFlow protocol on this interface.</td></tr> <tr> <td><i>tx</i></td><td>Monitor transmitted traffic on this interface.</td></tr> <tr> <td><i>rx</i></td><td>Monitor received traffic on this interface.</td></tr> <tr> <td><i>both</i></td><td>Monitor transmitted/received traffic on this interface.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable NetFlow protocol on this interface.	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.			
Option	Description													
<i>disable</i>	Disable NetFlow protocol on this interface.													
<i>tx</i>	Monitor transmitted traffic on this interface.													
<i>rx</i>	Monitor received traffic on this interface.													
<i>both</i>	Monitor transmitted/received traffic on this interface.													
sflow-sampler	Enable/disable sFlow on this interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sFlow protocol on this interface.</td></tr> <tr> <td><i>disable</i></td><td>Disable sFlow protocol on this interface.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable sFlow protocol on this interface.	<i>disable</i>	Disable sFlow protocol on this interface.							
Option	Description													
<i>enable</i>	Enable sFlow protocol on this interface.													
<i>disable</i>	Disable sFlow protocol on this interface.													
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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										

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>enable</i>	Enable source IP check.		
	<i>disable</i>	Disable source IP check.		
sample-rate	sFlow sample rate .	integer	Minimum value: 10 Maximum value: 99999	2000
polling-interval	sFlow polling interval .	integer	Minimum value: 1 Maximum value: 255	20
sample-direction	Data that NetFlow collects (rx, tx, or both).	option	-	both
	Option	Description		
	<i>tx</i>	Monitor transmitted traffic on this interface.		
	<i>rx</i>	Monitor received traffic on this interface.		
	<i>both</i>	Monitor transmitted/received traffic on this interface.		
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable
	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
	Option	Description		
	<i>enable</i>	Enable explicit FTP proxy on this interface.		
	<i>disable</i>	Disable explicit FTP proxy on this interface.		

Parameter	Description	Type	Size	Default
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable
	Option	Description		
	enable	Enable proxy captive portal on this interface.		
	disable	Disable proxy captive portal on this interface.		
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 0 Maximum value: 4294967295	0
inbandwidth	Bandwidth limit for incoming traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0
outbandwidth	Bandwidth limit for outgoing traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35	
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35	
disconnect-threshold	Time in milliseconds to wait before sending a notification that this interface is down or disconnected.	integer	Minimum value: 0 Maximum value: 10000	0
spillover-threshold	Egress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0
ingress-spillover-threshold	Ingress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0

Parameter	Description	Type	Size	Default
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
Option		Description		
		<i>enable</i>	Enable identifying the interface as an external interface.	
		<i>disable</i>	Disable identifying the interface as an external interface.	
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q
Option		Description		
		<i>8021q</i>	IEEE 802.1Q.	
		<i>8021ad</i>	IEEE 802.1AD.	
vlanid	VLAN ID .	integer	Minimum value: 1 Maximum value: 4094	0
trunk *	Enable/disable VLAN trunk.	option	-	disable
Option		Description		
		<i>enable</i>	Enable VLAN trunk on this interface.	
		<i>disable</i>	Disable VLAN trunk on this interface.	
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 Maximum value: 2147483647	0
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	

Parameter	Description	Type	Size	Default
lacp-mode	LACP mode.	option	-	active
	Option	Description		
	<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.		
	<i>passive</i>	Passively use LACP to negotiate 802.3ad aggregation.		
	<i>active</i>	Actively use LACP to negotiate 802.3ad aggregation.		
lacp-ha-slave	LACP HA slave.	option	-	enable
	Option	Description		
	<i>enable</i>	Allow HA slave to send/receive LACP messages.		
	<i>disable</i>	Block HA slave from sending/receiving LACP messages.		
lacp-speed	How often the interface sends LACP messages.	option	-	slow
	Option	Description		
	<i>slow</i>	Send LACP message every 30 seconds.		
	<i>fast</i>	Send LACP message every second.		
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
	Option	Description		
	<i>operational</i>	Set the aggregate operationally down.		
	<i>administrative</i>	Set the aggregate administratively down.		
algorithm	Frame distribution algorithm.	option	-	L4
	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.		

Parameter	Description	Type	Size	Default
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable
	Option	Description		
	enable	Enable fail back to higher priority port once recovered.		
	disable	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
vindex	Switch control interface VLAN ID.	integer	Minimum value: 0 Maximum value: 65535	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	
l2tp-client *	Enable/disable this interface as a Layer 2 Tunnelling Protocol (L2TP) client.	option	-	disable
	Option	Description		
	enable	Enable L2TP client.		
	disable	Disable L2TP client.		
security-mode	Turn on captive portal authentication for this interface.	option	-	none

Parameter	Description	Type	Size	Default
	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
	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-8021x-mode *	802.1X mode.	option	-	default
	Option	Description		
	<i>default</i>	802.1X default mode.		
	<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.		
	<i>fallback</i>	802.1X fallback (master) mode.		
	<i>slave</i>	802.1X slave mode.		
security-8021x-master *	802.1X master virtual-switch.	string	Maximum length: 15	
security-8021x-dynamic-vlan-id *	VLAN ID for virtual switch.	integer	Minimum value: 0 Maximum value: 4094	0
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	
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default	
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		
stp *	Enable/disable STP.	option	-	disable	
Option		Description			
		<i>disable</i>	Disable STP.		
		<i>enable</i>	Enable STP.		
stp-ha-secondary *	Control STP behaviour on HA secondary.	option	-	priority-adjust	
Option		Description			
		<i>disable</i>	Disable STP negotiation on HA secondary.		
		<i>enable</i>	Enable STP negotiation on HA secondary.		
		<i>priority-adjust</i>	Enable STP negotiation on HA secondary and make priority lower than HA primary.		
device-identification	Enable/disable passively gathering of device identity information about the devices on the network connected to this interface.	option	-	disable	
Option		Description			
		<i>enable</i>	Enable passive gathering of identity information about hosts.		
		<i>disable</i>	Disable passive gathering of identity information about hosts.		
device-user-identification	Enable/disable passive gathering of user identity information about users on this interface.	option	-	enable	
Option		Description			
		<i>enable</i>	Enable passive gathering of user identity information about users.		
		<i>disable</i>	Disable passive gathering of user identity information about users.		
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	vdom	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).		
	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).		
	<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	vdom
	Option	Description		
	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).		
	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).		
	<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.		
lldp-network-policy	LLDP-MED network policy profile.	string	Maximum length: 35	
estimated-upstream-bandwidth	Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295	0
estimated-downstream-bandwidth	Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295	0
measured-upstream-bandwidth	Measured upstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0
measured-downstream-bandwidth	Measured downstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default										
bandwidth-measure-time	Bandwidth measure time	integer	Minimum value: 0 Maximum value: 4294967295	0										
monitor-bandwidth	Enable monitoring bandwidth on this interface.	option	-	disable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable monitoring bandwidth on this interface.</td></tr> <tr> <td><i>disable</i></td><td>Disable monitoring bandwidth on this interface.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable monitoring bandwidth on this interface.	<i>disable</i>	Disable monitoring bandwidth on this interface.				
Option	Description													
<i>enable</i>	Enable monitoring bandwidth on this interface.													
<i>disable</i>	Disable monitoring bandwidth on this interface.													
vrrp-virtual-mac	Enable/disable use of virtual MAC for VRRP.	option	-	disable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable use of virtual MAC for VRRP.</td></tr> <tr> <td><i>disable</i></td><td>Disable use of virtual MAC for VRRP.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable use of virtual MAC for VRRP.	<i>disable</i>	Disable use of virtual MAC for VRRP.				
Option	Description													
<i>enable</i>	Enable use of virtual MAC for VRRP.													
<i>disable</i>	Disable use of virtual MAC for VRRP.													
role	Interface role.	option	-	undefined										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>lan</i></td><td>Connected to local network of endpoints.</td></tr> <tr> <td><i>wan</i></td><td>Connected to Internet.</td></tr> <tr> <td><i>dmz</i></td><td>Connected to server zone.</td></tr> <tr> <td><i>undefined</i></td><td>Interface has no specific role.</td></tr> </tbody> </table>					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.
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.													
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable secondary IP.</td></tr> <tr> <td><i>disable</i></td><td>Disable secondary IP.</td></tr> </tbody> </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.													
preserve-session-route	Enable/disable preservation of session route when dirty.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable preservation of session route when dirty.		
	disable	Disable preservation of session route when dirty.		
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension device on this interface.	option	-	disable
	Option	Description		
	enable	Enable automatic authorization of dedicated Fortinet extension device on this interface.		
	disable	Disable automatic authorization of dedicated Fortinet extension device on this interface.		
ap-discover	Enable/disable automatic registration of unknown FortiAP devices.	option	-	enable
	Option	Description		
	enable	Enable automatic registration of unknown FortiAP devices.		
	disable	Disable automatic registration of unknown FortiAP devices.		
fortilink-neighbor-detect	Protocol for FortiGate neighbor discovery.	option	-	fortilink
	Option	Description		
	lldp	Detect FortiLink neighbors using LLDP protocol.		
	fortilink	Detect FortiLink neighbors using FortiLink protocol.		
ip-managed-by-fortiipam	Enable/disable automatic IP address assignment of this interface by FortiIPAM.	option	-	disable
	Option	Description		
	enable	Enable automatic IP address assignment of this interface by FortiIPAM.		
	disable	Disable automatic IP address assignment of this interface by FortiIPAM.		
managed-subnetwork-size	Number of IP addresses to be allocated by FortiIPAM and used by this FortiGate unit's DHCP server settings.	option	-	256

Parameter	Description	Type	Size	Default
	Option	Description		
	256	Allocate a subnet with 256 IP addresses.		
	512	Allocate a subnet with 512 IP addresses.		
	1024	Allocate a subnet with 1024 IP addresses.		
	2048	Allocate a subnet with 2048 IP addresses.		
	4096	Allocate a subnet with 4096 IP addresses.		
	8192	Allocate a subnet with 8192 IP addresses.		
	16384	Allocate a subnet with 16384 IP addresses.		
	32768	Allocate a subnet with 32768 IP addresses.		
	65536	Allocate a subnet with 65536 IP addresses.		
fortilink-split-interface	Enable/disable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	option	-	enable
	Option	Description		
	enable	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.		
	disable	Disable FortiLink split interface.		
internal	Implicitly created.	integer	Minimum value: 0 Maximum value: 255	0
fortilink-backup-link	fortilink split interface backup link.	integer	Minimum value: 0 Maximum value: 255	0
switch-controller-access-vlan	Block FortiSwitch port-to-port traffic.	option	-	disable
	Option	Description		
	enable	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.		
	disable	Allow normal VLAN traffic.		

Parameter	Description	Type	Size	Default
switch-controller-traffic-policy	Switch controller traffic policy for the VLAN.	string	Maximum length: 63	
	Option	Description		
switch-controller-rspan-mode	Stop Layer2 MAC learning and interception of BPDUs and other packets on this interface.	option	-	disable
	Option	Description		
	disable	Disable RSPAN passthrough mode on this VLAN interface.		
	enable	Enable RSPAN passthrough mode on this VLAN interface.		
switch-controller-mgmt-vlan	VLAN to use for FortiLink management purposes.	integer	Minimum value: 1 Maximum value: 4094	4094
switch-controller-igmp-snooping	Switch controller IGMP snooping.	option	-	disable
	Option	Description		
	enable	Enable IGMP snooping.		
	disable	Disable IGMP snooping.		
switch-controller-igmp-snooping-proxy	Switch controller IGMP snooping proxy.	option	-	disable
	Option	Description		
	enable	Enable IGMP snooping proxy.		
	disable	Disable IGMP snooping proxy.		
switch-controller-igmp-snooping-fast-leave	Switch controller IGMP snooping fast-leave.	option	-	disable
	Option	Description		
	enable	Enable IGMP snooping fast-leave.		
	disable	Disable IGMP snooping fast-leave.		
switch-controller-dhcp-snooping	Switch controller DHCP snooping.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable DHCP snooping for FortiSwitch devices.		
	disable	Disable DHCP snooping for FortiSwitch devices.		
switch-controller-dhcp-snooping-verify-mac	Switch controller DHCP snooping verify MAC.	option	-	disable
	Option	Description		
	enable	Enable DHCP snooping verify source MAC for FortiSwitch devices.		
	disable	Disable DHCP snooping verify source MAC for FortiSwitch devices.		
switch-controller-dhcp-snooping-option82	Switch controller DHCP snooping option82.	option	-	disable
	Option	Description		
	enable	Enable DHCP snooping insert option82 for FortiSwitch devices.		
	disable	Disable DHCP snooping insert option82 for FortiSwitch devices.		
switch-controller-arp-inspection	Enable/disable FortiSwitch ARP inspection.	option	-	disable
	Option	Description		
	enable	Enable ARP inspection for FortiSwitch devices.		
	disable	Disable ARP inspection for FortiSwitch devices.		
switch-controller-learning-limit	Limit the number of dynamic MAC addresses on this VLAN .	integer	Minimum value: 0 Maximum value: 128	0
switch-controller-nac	Integrated FortiLink settings for managed FortiSwitch.	string	Maximum length: 35	
switch-controller-dynamic	Integrated FortiLink settings for managed FortiSwitch.	string	Maximum length: 35	
switch-controller-feature	Interface's purpose when assigning traffic (read only).	option	-	none
	Option	Description		
	none	VLAN for generic purpose.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default-vlan</i>	Default VLAN (native) assigned to all switch ports upon discovery.		
	<i>quarantine</i>	VLAN for quarantined traffic.		
	<i>rspan</i>	VLAN for RSPAN/ERSPAN mirrored traffic.		
	<i>voice</i>	VLAN dedicated for voice devices.		
	<i>video</i>	VLAN dedicated for camera devices.		
	<i>nac</i>	VLAN dedicated for NAC onboarding devices.		
	<i>nac-segment</i>	VLAN dedicated for NAC segment devices.		
switch-controller-iot-scanning	Enable/disable managed FortiSwitch IoT scanning.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IoT scanning for managed FortiSwitch devices.		
	<i>disable</i>	Disable IoT scanning for managed FortiSwitch devices.		
swc-vlan	Creation status for switch-controller VLANs.	integer	Minimum value: 0 Maximum value: 4294967295	0
swc-first-create	Initial create for switch-controller VLANs.	integer	Minimum value: 0 Maximum value: 4294967295	0
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

* This parameter may not exist in some models.

** Values may differ between models.

config client-options

Parameter	Description	Type	Size	Default
code	DHCP client option code.	integer	Minimum value: 0 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 l2tp-client-settings

Parameter	Description	Type	Size	Default
user	L2TP user name.	string	Maximum length: 127	
password	L2TP password.	password	Not Specified	
peer-host	L2TP peer host address.	string	Maximum length: 255	
peer-mask	L2TP peer mask.	ipv4-netmask	Not Specified	255.255.255.255
peer-port	L2TP peer port number.	integer	Minimum value: 1 Maximum value: 65535	1701
auth-type	L2TP authentication type.	option	-	auto
Option		Description		
		<i>auto</i> Automatically choose authentication.		
		<i>pap</i> PAP authentication.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
mtu	L2TP MTU.	integer	Minimum value: 40 Maximum value: 65535	1460
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255	2
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295	0
defaultgw	Enable/disable default gateway.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable default gateway.		
	<i>disable</i>	Disable default gateway.		
ip	IP.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0

config vrrp

Parameter	Description	Type	Size	Default
version	VRRP version.	option	-	2
	Option	Description		
	2	VRRP version 2.		
	3	VRRP version 3.		

Parameter	Description	Type	Size	Default						
vrgrp	VRRP group ID .	integer	Minimum value: 1 Maximum value: 65535	0						
vrip	IP address of the virtual router.	ipv4-address-any	Not Specified	0.0.0.0						
priority	Priority of the virtual router .	integer	Minimum value: 1 Maximum value: 255	100						
adv-interval	Advertisement interval .	integer	Minimum value: 1 Maximum value: 255	1						
start-time	Startup time .	integer	Minimum value: 1 Maximum value: 255	3						
preempt	Enable/disable preempt mode.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable preempt mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable preempt mode.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable preempt mode.	<i>disable</i>	Disable preempt mode.
Option	Description									
<i>enable</i>	Enable preempt mode.									
<i>disable</i>	Disable preempt mode.									
accept-mode	Enable/disable accept mode.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable accept mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable accept mode.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable accept mode.	<i>disable</i>	Disable accept mode.
Option	Description									
<i>enable</i>	Enable accept mode.									
<i>disable</i>	Disable accept mode.									
vrdst	Monitor the route to this destination.	ipv4-address-any	Not Specified							
vrdst-priority	Priority of the virtual router when the virtual router destination becomes unreachable .	integer	Minimum value: 0 Maximum value: 254	0						
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ignoring of default route when checking destination.		
	<i>disable</i>	Disable ignoring of default route when checking destination.		
status	Enable/disable this VRRP configuration.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this VRRP configuration.		
	<i>disable</i>	Disable this VRRP configuration.		

config proxy-arp

Parameter	Description	Type	Size	Default
ip	Set IP addresses of proxy ARP.	user	Not Specified	

config secondaryip

Parameter	Description	Type	Size	Default
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified	0.0.0.0
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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 dhcp-snooping-server-list

Parameter	Description	Type	Size	Default
server-ip	IP address for DHCP server.	ipv4-address	Not Specified	0.0.0.0

config tagging

Parameter	Description	Type	Size	Default
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										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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 .	integer	Minimum value: 0 Maximum value: 7	0										
nd-timestamp-delta	Neighbor discovery timestamp delta value .	integer	Minimum value: 1 Maximum value: 3600	300										
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor .	integer	Minimum value: 1 Maximum value: 60	1										

Parameter	Description	Type	Size	Default
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
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:xxx/xxx	ipv6-prefix	Not Specified	::/0
ip6-allowaccess	Allow management access to the interface.	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>fabric</i> Fabric access.		
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-	disable
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
Option		Description		
		<i>enable</i> Enable sending of ICMPv6 redirects.		
		<i>disable</i> Disable sending of ICMPv6 redirects.		

Parameter	Description	Type	Size	Default
ip6-manage-flag	Enable/disable the managed flag.	option	-	disable
	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
	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
	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

Parameter	Description	Type	Size	Default						
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						
autoconf	Enable/disable address auto config.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable auto-configuration.</td></tr> <tr> <td><i>disable</i></td><td>Disable auto-configuration.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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-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/xxx	ipv6-prefix	Not Specified	::/0						
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable DHCPv6 relay</td></tr> <tr> <td><i>enable</i></td><td>Enable DHCPv6 relay.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>regular</i></td><td>Regular DHCP relay.</td></tr> </tbody> </table>				Option	Description	<i>regular</i>	Regular DHCP relay.				
Option	Description											
<i>regular</i>	Regular DHCP relay.											
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified									
dhcp6-client-options	DHCPv6 client options.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </table>				Option	Description	<i>enable</i>	Enable DHCPv6 prefix delegation.	<i>disable</i>	Disable DHCPv6 prefix delegation.		
Option	Description											
<i>enable</i>	Enable DHCPv6 prefix delegation.											
<i>disable</i>	Disable DHCPv6 prefix delegation.											
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											
dhcp6-prefix-hint	DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.	ipv6-network	Not Specified	::/0								
dhcp6-prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 Maximum value: 4294967295	604800								

Parameter	Description	Type	Size	Default
dhcp6-prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000
cli-conn6-status	CLI IPv6 connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0
vrrp-virtual-mac6	Enable/disable virtual MAC for VRRP.	option	-	disable
Option		Description		
		<i>enable</i> Enable virtual MAC for VRRP.		
		<i>disable</i> Disable virtual MAC for VRRP.		
vrip6_link_local	Link-local IPv6 address of virtual router.	ipv6-address	Not Specified	::

config ip6-prefix-list

Parameter	Description	Type	Size	Default
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.		
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000

Parameter	Description	Type	Size	Default
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
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15	
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.		
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 vrrp6

Parameter	Description	Type	Size	Default						
vrgrp	VRRP group ID .	integer	Minimum value: 1 Maximum value: 65535	0						
vrip6	IPv6 address of the virtual router.	ipv6-address	Not Specified	::						
priority	Priority of the virtual router .	integer	Minimum value: 1 Maximum value: 255	100						
adv-interval	Advertisement interval .	integer	Minimum value: 1 Maximum value: 255	1						
start-time	Startup time .	integer	Minimum value: 1 Maximum value: 255	3						
preempt	Enable/disable preempt mode.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable preempt mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable preempt mode.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable preempt mode.	<i>disable</i>	Disable preempt mode.
Option	Description									
<i>enable</i>	Enable preempt mode.									
<i>disable</i>	Disable preempt mode.									
accept-mode	Enable/disable accept mode.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable accept mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable accept mode.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable accept mode.	<i>disable</i>	Disable accept mode.
Option	Description									
<i>enable</i>	Enable accept mode.									
<i>disable</i>	Disable accept mode.									
vrdst6	Monitor the route to this destination.	ipv6-address	Not Specified							
status	Enable/disable VRRP.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable VRRP.</td></tr> <tr> <td><i>disable</i></td><td>Disable VRRP.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable VRRP.	<i>disable</i>	Disable VRRP.
Option	Description									
<i>enable</i>	Enable VRRP.									
<i>disable</i>	Disable VRRP.									

config system physical-switch



This command is available for reference model(s) FortiGate 140E-POE, FortiWiFi 61F. It is not available for FortiGate 501E, FortiGate 3000D, FortiGate VM64.

Configure physical switches.

```
config system physical-switch
  Description: Configure physical switches.
  edit <name>
    set age-enable {enable|disable}
    set age-val {integer}
  next
end
```

config system physical-switch

Parameter	Description	Type	Size	Default
age-enable	Enable/disable layer 2 age timer.	option	-	disable
age-val	Layer 2 table age timer value.	integer	Minimum value: 0 Maximum value: 4294967295	3158067

config system virtual-switch



This command is available for reference model(s) FortiGate 140E-POE, FortiWiFi 61F. It is not available for FortiGate 501E, FortiGate 3000D, FortiGate VM64.

Configure virtual hardware switch interfaces.

```
config system virtual-switch
  Description: Configure virtual hardware switch interfaces.
  edit <name>
    set physical-switch {string}
    set vlan {integer}
    config port
      Description: Configure member ports.
      edit <name>
```

```

        set alias {string}
        set poe [enable|disable]
    next
end
set span [disable|enable]
set span-source-port {string}
set span-dest-port {string}
set span-direction [rx|tx|...]
next
end

```

config system virtual-switch

Parameter	Description	Type	Size	Default
physical-switch	Physical switch parent.	string	Maximum length: 15	
vlan *	VLAN.	integer	Minimum value: 0 Maximum value: 4294967295	0
span	Enable/disable SPAN.	option	-	disable
Option	Description			
<i>disable</i>	Disable SPAN.			
<i>enable</i>	Enable SPAN.			
span-source-port	SPAN source port.	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.			

* This parameter may not exist in some models.

config port

Parameter	Description	Type	Size	Default
alias	Alias.	string	Maximum length: 25	
poe *	Enable/disable PoE status.	option	-	enable
		Option	Description	
		enable	Enable PoE status.	
		disable	Disable PoE status.	

* This parameter may not exist in some models.

config system stp



This command is available for reference model(s) FortiGate 140E-POE, FortiWiFi 61F. It is not available for FortiGate 501E, FortiGate 3000D, FortiGate VM64.

Configure Spanning Tree Protocol (STP).

```
config system stp
  Description: Configure Spanning Tree Protocol (STP).
  set switch-priority [0|4096|...]
  set hello-time {integer}
  set forward-delay {integer}
  set max-age {integer}
  set max-hops {integer}
end
```

config system stp

Parameter	Description	Type	Size	Default
switch-priority	STP switch priority; the lower the number the higher the priority (select from 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, and 57344).	option	-	32768
		Option	Description	
		0	0	
		4096	4096	
		8192	8192	

Parameter	Description	Type	Size	Default
	Option	Description		
	12288	12288		
	16384	16384		
	20480	20480		
	24576	24576		
	28672	28672		
	32768	32768		
	36864	36864		
	40960	40960		
	45056	45056		
	49152	49152		
	53248	53248		
	57344	57344		
hello-time	Hello time .	integer	Minimum value: 1 Maximum value: 10	2
forward-delay	Forward delay .	integer	Minimum value: 4 Maximum value: 30	15
max-age	Maximum packet age .	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops .	integer	Minimum value: 1 Maximum value: 40	20

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]
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
	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
	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 .	integer	Minimum value: 8 Maximum value: 128	8
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0

Parameter	Description	Type	Size	Default						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password .	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 (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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.									

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]
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
	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
	Option	Description		
	<i>guest-admin-password</i>	Apply to guest administrator password.		
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128	8
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128	0

Parameter	Description	Type	Size	Default
min-change-characters	Minimum number of unique characters in new password which do not exist in old password (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
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 .	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.		

config system sms-server

Configure SMS server for sending SMS messages to support user authentication.

```
config system sms-server
  Description: Configure SMS server for sending SMS messages to support user authentication.
  edit <name>
    set mail-server {string}
  next
end
```

config system sms-server

Parameter	Description	Type	Size	Default
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	

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
filename	Custom language file path.	string	Maximum length: 63	
comments	Comment.	var-string	Maximum length: 255	

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 radius-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}
next
end

```

config system admin

Parameter	Description	Type	Size	Default
wildcard	Enable/disable wildcard RADIUS authentication.	option	-	disable
	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
	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

Parameter	Description	Type	Size	Default
	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 FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost2	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost3	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost4	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost5	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost6	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost7	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost8	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
trusthost9	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost10	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost2	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost3	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost4	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost5	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost6	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost8	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost9	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost10	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiGate features.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable allow-remove option.		
	<i>disable</i>	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 FortiGate 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 FortiGate features that this administrator can access.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable access profile override.		
	<i>disable</i>	Disable access profile override.		
radius-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

Parameter	Description	Type	Size	Default
	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	-	
	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.		

Parameter	Description	Type	Size	Default
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
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
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 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
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			
<i>enable</i>	Enable peer.			
<i>disable</i>	Disable peer.			
peer-group	Peer group name.	string	Maximum length: 35	

config trusthost

Parameter	Description	Type	Size	Default
type	Trusthost type.	option	-	ipv4-trusthost
Option	Description			
<i>ipv4-trusthost</i>	IPv4 trusthost.			
<i>ipv6-trusthost</i>	IPv6 trusthost.			

Parameter	Description	Type	Size	Default
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified	0.0.0.0
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified	::/0

config system sso-admin

Configure SSO admin users.

```
config system sso-admin
  Description: Configure SSO admin users.
  edit <name>
    set accprofile {string}
    set vdom <name1>, <name2>, ...
  next
end
```

config system sso-admin

Parameter	Description	Type	Size	Default
accprofile	SSO admin user access profile.	string	Maximum length: 35	
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 vdom <name1>, <name2>, ...
  next
end
```

config system sso-forticloud-admin

Parameter	Description	Type	Size	Default
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system settings

Configure VDOM settings.

```
config system settings
  Description: Configure VDOM settings.
  set comments {var-string}
  set opmode [nat|transparent]
  set ngfw-mode [profile-based|policy-based]
  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 bfd [enable|disable]
  set bfd-desired-min-tx {integer}
  set bfd-required-min-rx {integer}
  set bfd-detect-mult {integer}
  set bfd-dont-enforce-src-port [enable|disable]
  set utf8-spam-tagging [enable|disable]
  set wccp-cache-engine [enable|disable]
  set vpn-stats-log {option1}, {option2}, ...
  set vpn-stats-period {integer}
  set v4-ecmp-mode [source-ip-based|weight-based|...]
  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|sdwan|...]
  set dhcp-proxy-interface {string}
  set dhcp-server-ip {user}
  set dhcp6-server-ip {user}
  set central-nat [enable|disable]
  set gui-default-policy-columns <name1>, <name2>, ...
  set lldp-reception [enable|disable|...]
  set lldp-transmission [enable|disable|...]
  set link-down-access [enable|disable]
  set auxiliary-session [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 sip-expectation [enable|disable]
  set sip-nat-trace [enable|disable]
  set status [enable|disable]
  set sip-tcp-port {integer}
  set sip-udp-port {integer}
```

```
set sip-ssl-port {integer}
set sccp-port {integer}
set multicast-forward [enable|disable]
set multicast-ttl-notchange [enable|disable]
set multicast-skip-policy [enable|disable]
set allow-subnet-overlap [enable|disable]
set deny-tcp-with-icmp [enable|disable]
set ecmp-max-paths {integer}
set discovered-device-timeout {integer}
set email-portal-check-dns [disable|enable]
set default-voip-alg-mode [proxy-based|kernel-helper-based]
set gui-icap [enable|disable]
set gui-implicit-policy [enable|disable]
set gui-dns-database [enable|disable]
set gui-load-balance [enable|disable]
set gui-multicast-policy [enable|disable]
set gui-dos-policy [enable|disable]
set gui-object-colors [enable|disable]
set gui-voip-profile [enable|disable]
set gui-ap-profile [enable|disable]
set gui-security-profile-group [enable|disable]
set gui-local-in-policy [enable|disable]
set gui-explicit-proxy [enable|disable]
set gui-dynamic-routing [enable|disable]
set gui-sslvpn-personal-bookmarks [enable|disable]
set gui-sslvpn-realms [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-wireless-controller [enable|disable]
set gui-switch-controller [enable|disable]
set gui-fortiapi-split-tunneling [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-wan-load-balancing [enable|disable]
set gui-antivirus [enable|disable]
set gui-webfilter [enable|disable]
set gui-videofilter [enable|disable]
set gui-dnsfilter [enable|disable]
set gui-waf-profile [enable|disable]
set gui-fortiextender-controller [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 location-id {ipv4-address}
set ike-session-resume [enable|disable]
set ike-quick-crash-detect [enable|disable]
```

```

set ike-dn-format [with-space|no-space]
set ike-port {integer}
set block-land-attack [disable|enable]
set application-bandwidth-tracking [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
	Option	Description		
	<i>nat</i>	Change to NAT mode.		
	<i>transparent</i>	Change to transparent mode.		
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-	profile-based
	Option	Description		
	<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.		
	<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.		
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.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<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	
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		
bfd	Enable/disable Bi-directional Forwarding Detection (BFD) on all interfaces.	option	-	enable	disable
	Option	Description			
	<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.			
	<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.			
bfd-desired-min-tx	BFD desired minimal transmit interval .	integer	Minimum value: 1 Maximum value: 100000	250	
bfd-required-min-rx	BFD required minimal receive interval .	integer	Minimum value: 1 Maximum value: 100000	250	
bfd-detect-mult	BFD detection multiplier .	integer	Minimum value: 1 Maximum value: 50	3	
bfd-dont-enforce-src-port	Enable to not enforce verifying the source port of BFD Packets.	option	-	enable	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable verifying the source port of BFD Packets.		
	<i>disable</i>	Disable verifying the source port of BFD Packets.		
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-	enable
	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
	Option	Description		
	<i>enable</i>	Enable WCCP cache engine.		
	<i>disable</i>	Disable WCCP cache engine.		
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-	ipsec pptp l2tp ssl
	Option	Description		
	<i>ipsec</i>	IPsec.		
	<i>pptp</i>	PPTP.		
	<i>l2tp</i>	L2TP.		
	<i>ssl</i>	SSL.		
vpn-stats-period	Period to send VPN log statistics .	integer	Minimum value: 0 Maximum value: 4294967295	600
v4-ecmp-mode	IPv4 Equal-cost multi-path (ECMP) routing and load balancing mode.	option	-	source-ip-based
	Option	Description		
	<i>source-ip-based</i>	Select next hop based on source IP.		
	<i>weight-based</i>	Select next hop based on weight.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>usage-based</i>	Select next hop based on usage.		
	<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.		
mac-ttl	Duration of MAC addresses in Transparent mode .	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 FortiGate.	option	-	disable
	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
	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
	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
	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
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
dhcp-proxy-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	
central-nat	Enable/disable central NAT.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable central NAT.		
	<i>disable</i>	Disable central NAT.		
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79	
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception for this VDOM or apply global settings to this VDOM.	option	-	global
	Option	Description		
	<i>enable</i>	Enable LLDP reception for this VDOM.		
	<i>disable</i>	Disable LLDP reception for this VDOM.		
	<i>global</i>	Use the global LLDP reception configuration for this VDOM.		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission for this VDOM or apply global settings to this VDOM.	option	-	global
	Option	Description		
	<i>enable</i>	Enable LLDP transmission for this VDOM.		
	<i>disable</i>	Disable LLDP transmission for this VDOM.		
	<i>global</i>	Use the global LLDP transmission configuration for this VDOM.		
link-down-access	Enable/disable link down access traffic.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Allow link down access traffic.		
	<i>disable</i>	Block link down access traffic.		
auxiliary-session	Enable/disable auxiliary session.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable auxiliary session for this VDOM.		
	<i>disable</i>	Disable auxiliary session for this VDOM.		
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv4 asymmetric routing.		
	<i>disable</i>	Disable IPv4 asymmetric routing.		
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ICMP asymmetric routing.		
	<i>disable</i>	Disable ICMP asymmetric routing.		
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable
	Option	Description		
	<i>enable</i>	Allow TCP session without SYN flags.		
	<i>disable</i>	Do not allow TCP session without SYN flags.		
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable
	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

Parameter	Description	Type	Size	Default
	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
	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
	Option	Description		
	<i>enable</i>	Enable asymmetric IPv6 routing.		
	<i>disable</i>	Disable asymmetric IPv6 routing.		
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable asymmetric ICMPv6 routing.		
	<i>disable</i>	Disable asymmetric ICMPv6 routing.		
sctp-session-without-init	Enable/disable SCTP session creation without SCTP INIT.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SCTP session creation without SCTP INIT.		
	<i>disable</i>	Disable SCTP session creation without SCTP INIT.		
sip-expectation	Enable/disable the SIP kernel session helper to create an expectation for port 5060.	option	-	disable
	Option	Description		
	<i>enable</i>	Allow SIP session helper to create an expectation for port 5060.		
	<i>disable</i>	Prevent SIP session helper from creating an expectation for port 5060.		
sip-nat-trace	Enable/disable recording the original SIP source IP address when NAT is used.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Record the original SIP source IP address when NAT is used.		
	<i>disable</i>	Do not record the original SIP source IP address when NAT is used.		
status	Enable/disable this VDOM.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this VDOM.		
	<i>disable</i>	Disable this VDOM.		
sip-tcp-port	TCP port the SIP proxy monitors for SIP traffic .	integer	Minimum value: 1 Maximum value: 65535	5060
sip-udp-port	UDP port the SIP proxy monitors for SIP traffic .	integer	Minimum value: 1 Maximum value: 65535	5060
sip-ssl-port	TCP port the SIP proxy monitors for SIP SSL/TLS traffic .	integer	Minimum value: 0 Maximum value: 65535	5061
sccp-port	TCP port the SCCP proxy monitors for SCCP traffic .	integer	Minimum value: 0 Maximum value: 65535	2000
multicast-forward	Enable/disable multicast forwarding.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast forwarding.		
	<i>disable</i>	Disable multicast forwarding.		
multicast-ttl-notchange	Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.	option	-	disable
	Option	Description		
	<i>enable</i>	The multicast TTL is not changed.		
	<i>disable</i>	The multicast TTL may be changed.		

Parameter	Description	Type	Size	Default
multicast-skip-policy	Enable/disable allowing multicast traffic through the FortiGate without a policy check.	option	-	disable
	Option	Description		
	<i>enable</i>	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.		
	<i>disable</i>	Require a multicast policy to allow multicast traffic to pass through the FortiGate.		
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.		
ecmp-max-paths	Maximum number of Equal Cost Multi-Path .	integer	Minimum value: 1 Maximum value: 255	255
discovered-device-timeout	Timeout for discovered devices .	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.		
default-voip-alg-mode	Configure how the FortiGate handles VoIP traffic when a policy that accepts the traffic doesn't include a VoIP profile.	option	-	proxy-based

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>proxy-based</i>	Use a default proxy-based VoIP ALG.		
	<i>kernel-helper-based</i>	Use the SIP session helper.		
gui-icap	Enable/disable ICAP on the GUI.	option	-	disable
	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-load-balance	Enable/disable server load balancing on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable server load balancing on the GUI.		
	<i>disable</i>	Disable server load balancing 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	-	enable **

Parameter	Description	Type	Size	Default
	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-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-ap-profile	Enable/disable FortiAP profiles on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiAP profiles on the GUI.		
	<i>disable</i>	Disable FortiAP profiles on the GUI.		
gui-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-local-in-policy	Enable/disable Local-In policies on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Local-In policies on the GUI.		
	<i>disable</i>	Disable Local-In policies on the GUI.		
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
		<i>enable</i>		Enable the explicit proxy on the GUI.
		<i>disable</i>		Disable the explicit proxy on the GUI.
gui-dynamic-routing	Enable/disable dynamic routing on the GUI.	option	-	enable **
	Option	Description		
		<i>enable</i>		Enable dynamic routing on the GUI.
		<i>disable</i>		Disable dynamic routing on the GUI.
gui-ssvpn-personal-bookmarks	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-	disable
	Option	Description		
		<i>enable</i>		Enable SSL-VPN personal bookmark management on the GUI.
		<i>disable</i>		Disable SSL-VPN personal bookmark management on the GUI.
gui-ssvpn-realms	Enable/disable SSL-VPN realms on the GUI.	option	-	disable
	Option	Description		
		<i>enable</i>		Enable SSL-VPN realms on the GUI.
		<i>disable</i>		Disable SSL-VPN realms on the GUI.
gui-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
	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

Parameter	Description	Type	Size	Default
	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	-	disable **
	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	-	enable
	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
	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

Parameter	Description	Type	Size	Default
	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 VPN tunnels on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VPN tunnels on the GUI.		
	<i>disable</i>	Disable VPN tunnels on the GUI.		
gui-wireless-controller	Enable/disable the wireless controller on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the wireless controller on the GUI.		
	<i>disable</i>	Disable the wireless controller on the GUI.		
gui-switch-controller	Enable/disable the switch controller on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the switch controller on the GUI.		
	<i>disable</i>	Disable the switch controller on the GUI.		
gui-fortiap-split-tunneling	Enable/disable FortiAP split tunneling on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiAP split tunneling on the GUI.		
	<i>disable</i>	Disable FortiAP split tunneling on the GUI.		
gui-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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable traffic shaping on the GUI.		
	<i>disable</i>	Disable traffic shaping on the GUI.		
gui-wan-load-balancing	Enable/disable SD-WAN on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SD-WAN on the GUI.		
	<i>disable</i>	Disable SD-WAN on the GUI.		
gui-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
	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-waf-profile	Enable/disable Web Application Firewall on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Web Application Firewall on the GUI.		
	<i>disable</i>	Disable Web Application Firewall on the GUI.		
gui-fortiextender-controller	Enable/disable FortiExtender on the GUI.	option	-	enable **
	Option	Description		
	<i>enable</i>	Enable FortiExtender on the GUI.		
	<i>disable</i>	Disable FortiExtender 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.		
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the requirement for policy naming on the GUI.		
	<i>disable</i>	Disable the requirement for policy naming on the GUI.		
gui-email-collection	Enable/disable email collection on the GUI.	option	-	disable
	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
	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.		

Parameter	Description	Type	Size	Default
gui-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-	disable
	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
	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.		
location-id	Local location ID in the form of an IPv4 address.	ipv4-address	Not Specified	0.0.0.0
ike-session-resume	Enable/disable IKEv2 session resumption (RFC 5723).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).		
	<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).		
ike-quick-crash-detect	Enable/disable IKE quick crash detection (RFC 6290).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IKE quick crash detection (RFC 6290).		
	<i>disable</i>	Disable IKE quick crash detection (RFC 6290).		
ike-dn-format	Configure IKE ASN.1 Distinguished Name format conventions.	option	-	with-space
	Option	Description		
	<i>with-space</i>	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.		
	<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.		

Parameter	Description	Type	Size	Default						
ike-port	UDP port for IKE/IPsec traffic .	integer	Minimum value: 1024 Maximum value: 65535	500						
block-land-attack	Enable/disable blocking of land attacks.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>disable</td><td>Do not block land attack.</td></tr> <tr> <td>enable</td><td>Block land attack.</td></tr> </tbody> </table>	Option	Description	disable	Do not block land attack.	enable	Block land attack.			
Option	Description									
disable	Do not block land attack.									
enable	Block land attack.									
application-bandwidth-tracking	Enable/disable application bandwidth tracking.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>disable</td><td>Disable application bandwidth tracking.</td></tr> <tr> <td>enable</td><td>Enable application bandwidth tracking.</td></tr> </tbody> </table>	Option	Description	disable	Disable application bandwidth tracking.	enable	Enable application bandwidth tracking.			
Option	Description									
disable	Disable application bandwidth tracking.									
enable	Enable application bandwidth tracking.									

** Values may differ between models.

config system sit-tunnel

Configure IPv6 tunnel over IPv4.

```
config system sit-tunnel
  Description: Configure IPv6 tunnel over IPv4.
  edit <name>
    set source {ipv4-address}
    set destination {ipv4-address}
    set ip6 {ipv6-prefix}
    set interface {string}
    set use-sdwan [disable|enable]
    set auto-asic-offload [enable|disable]
  next
end
```

config system sit-tunnel

Parameter	Description	Type	Size	Default
source	Source IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0
destination	Destination IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
ip6	IPv6 address of the tunnel.	ipv6-prefix	Not Specified	::/0
interface	Interface name.	string	Maximum length: 15	
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
	Option	Description		
	disable	Disable use of SD-WAN to reach remote gateway.		
	enable	Enable use of SD-WAN to reach remote gateway.		
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	Option	Description		
	enable	Enable auto ASIC offloading.		
	disable	Disable ASIC offloading.		

* This parameter may not exist in some models.

config system fss-o-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fss-o-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 fss-o-polling

Parameter	Description	Type	Size	Default
status	Enable/disable FSSO Polling Mode.	option	-	enable
	Option	Description		
	enable	Enable FSSO Polling Mode.		
	disable	Disable FSSO Polling Mode.		

Parameter	Description	Type	Size	Default
listening-port	Listening port to accept clients .	integer	Minimum value: 1 Maximum value: 65535	8000
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable
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 ha

Configure HA.

```
config system ha
  Description: Configure HA.
  set group-id {integer}
  set group-name {string}
  set mode [standalone|a-a|...]
  set sync-packet-balance [enable|disable]
  set password {password}
  set key {password}
  set hbdev {user}
  set session-sync-dev {user}
  set route-ttl {integer}
  set route-wait {integer}
  set route-hold {integer}
  set multicast-ttl {integer}
  set load-balance-all [enable|disable]
  set sync-config [enable|disable]
  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 session-pickup [enable|disable]
  set session-pickup-connectionless [enable|disable]
  set session-pickup-expectation [enable|disable]
  set session-pickup-nat [enable|disable]
  set session-pickup-delay [enable|disable]
  set link-failed-signal [enable|disable]
  set uninterrupted-upgrade [enable|disable]
```

```
set standalone-mgmt-vdom [enable|disable]
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-eth-type {string}
set hc-eth-type {string}
set l2ep-eth-type {string}
set ha-upptime-diff-margin {integer}
set standalone-config-sync [enable|disable]
set logical-sn [enable|disable]
set vcluster-id {integer}
set override [enable|disable]
set priority {integer}
set override-wait-time {integer}
set schedule [none|hub|...]
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 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 {user}
set vcluster2 [enable|disable]
config secondary-vcluster
    Description: Configure virtual cluster 2.
    set vcluster-id {integer}
    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 vdom {user}
end
set ha-direct [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}
end

```

config system ha

Parameter	Description	Type	Size	Default
group-id	HA group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255	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
Option		Description		
		<i>standalone</i> Standalone mode.		
		<i>a-a</i> Active-active mode.		
		<i>a-p</i> Active-passive mode.		
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable
Option		Description		
		<i>enable</i> Enable HA packet distribution to multiple CPUs.		
		<i>disable</i> Disable HA packet distribution to multiple CPUs.		
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	
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified	
route-ttl	TTL for primary unit routes . 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 .	integer	Minimum value: 0 Maximum value: 3600	0

Parameter	Description	Type	Size	Default						
route-hold	Time to wait between routing table updates to the cluster .	integer	Minimum value: 0 Maximum value: 3600	10						
multicast-ttl	HA multicast TTL on primary .	integer	Minimum value: 5 Maximum value: 3600	600						
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable load balance.</td></tr> <tr> <td><i>disable</i></td><td>Disable load balance.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable load balance.	<i>disable</i>	Disable load balance.			
Option	Description									
<i>enable</i>	Enable load balance.									
<i>disable</i>	Disable load balance.									
sync-config	Enable/disable configuration synchronization.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable configuration synchronization.</td></tr> <tr> <td><i>disable</i></td><td>Disable configuration synchronization.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable configuration synchronization.	<i>disable</i>	Disable configuration synchronization.			
Option	Description									
<i>enable</i>	Enable configuration synchronization.									
<i>disable</i>	Disable configuration synchronization.									
encryption	Enable/disable heartbeat message encryption.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2						
hb-interval-in-milliseconds	Number of milliseconds for each heartbeat interval: 100ms or 10ms.	option	-	100ms						

Parameter	Description	Type	Size	Default
	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 . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	6 **
hello-holddown	Time to wait before changing from hello to work state .	integer	Minimum value: 5 Maximum value: 300	20
gratuitous-arpss	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 . Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60	5
arps-interval	Time between gratuitous ARPs . Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20	8
session-pickup	Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.	option	-	disable
	Option	Description		
	enable	Enable session pickup.		
	disable	Disable session pickup.		
session-pickup-connectionless	Enable/disable UDP and ICMP session sync.	option	-	disable
	Option	Description		
	enable	Enable setting.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
session-pickup-expectation	Enable/disable session helper expectation session sync for FGSP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
session-pickup-nat	Enable/disable NAT session sync for FGSP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
session-pickup-delay	Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
standalone-mgmt-vdom	Enable/disable standalone management VDOM.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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-eth-type	HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8890
hc-eth-type	Transparent mode HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8891
l2ep-eth-type	Telnet session HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8893
ha-upptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535	300
standalone-config-sync	Enable/disable FGSP configuration synchronization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
logical-sn	Enable/disable usage of the logical serial number.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable usage of the logical serial number.		
	<i>disable</i>	Disable usage of the logical serial number.		
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
override	Enable and increase the priority of the unit that should always be primary.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
schedule	Type of A-A load balancing. Use none if you have external load balancers.	option	-	round-robin
	Option	Description		
	<i>none</i>	None.		
	<i>hub</i>	Hub.		
	<i>leastconnection</i>	Least connection.		
	<i>round-robin</i>	Round robin.		
	<i>weight-round-robin</i>	Weight round robin.		
	<i>random</i>	Random.		
	<i>ip</i>	IP.		
	<i>ipport</i>	IP port.		
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	

Parameter	Description	Type	Size	Default
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified	
nntp-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	
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified	
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 .	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 after PING server failure.			
<i>disable</i>	Disable force reset of secondary after PING server failure.			
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	VDOMs in virtual cluster 1.	user	Not Specified	
vcluster2	Enable/disable virtual cluster 2 for virtual clustering.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			

Parameter	Description	Type	Size	Default						
ha-direct	Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.</td></tr> <tr> <td><i>disable</i></td><td>Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.	<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.			
Option	Description									
<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.									
<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.									
memory-compatible-mode	Enable/disable memory compatible mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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-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 .	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 .	integer	Minimum value: 1 Maximum value: 60	1						
memory-failover-flip-timeout	Time to wait between subsequent memory based failovers in minutes .	integer	Minimum value: 6 Maximum value: 2147483647	6						

Parameter	Description	Type	Size	Default
failover-hold-time	Time to wait before failover , to avoid flip.	integer	Minimum value: 0 Maximum value: 300	0

** Values may differ between models.

config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
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 secondary-vcluster

Parameter	Description	Type	Size	Default
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	1
override	Enable and increase the priority of the unit that should always be primary.	option	-	enable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0

Parameter	Description	Type	Size	Default
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 .	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		
	enable	Enable force reset of secondary after PING server failure.		
	disable	Disable force reset of secondary after PING server failure.		
vdom	VDOMs in virtual cluster 2.	user	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		
	enable	Enable monitor VLAN interfaces.		
	disable	Disable monitor VLAN interfaces.		

Parameter	Description	Type	Size	Default
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30	5
vlan-hb-lost-threshold	VLAN lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 60	3

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 {option}
  next
end
```

config system storage

Parameter	Description	Type	Size	Default								
status	Enable/disable storage.	option	-	enable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
media-status	The physical status of current media.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Storage is enabled.</td></tr> <tr> <td><i>disable</i></td><td>Storage is disabled.</td></tr> <tr> <td><i>fail</i></td><td>Storage have some fail sector.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Storage is enabled.	<i>disable</i>	Storage is disabled.	<i>fail</i>	Storage have some fail sector.
Option	Description											
<i>enable</i>	Storage is enabled.											
<i>disable</i>	Storage is disabled.											
<i>fail</i>	Storage have some fail sector.											

Parameter	Description	Type	Size	Default
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 and WAN Optimization.	option	-	log
Option	Description			
<i>log</i>	Use hard disk for logging.			

config system dedicated-mgmt

Configure dedicated management.

```
config system dedicated-mgmt
  Description: Configure dedicated management.
  set status [enable|disable]
  set interface {string}
  set default-gateway {ipv4-address}
  set dhcp-server [enable|disable]
  set dhcp-netmask {ipv4-netmask}
  set dhcp-start-ip {ipv4-address}
  set dhcp-end-ip {ipv4-address}
end
```

config system dedicated-mgmt

Parameter	Description	Type	Size	Default
status	Enable/disable dedicated management.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			

Parameter	Description	Type	Size	Default
interface	Dedicated management interface.	string	Maximum length: 15	
	Option	Description		
	<i>enable</i>	Enable DHCP server on management port.		
	<i>disable</i>	Disable DHCP server on management port.		
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified	0.0.0.0
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0

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
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 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
interface	Select the associated interface name from available options.	string	Maximum length: 15	
ipv6	IPv6 address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
mac	MAC address (format: xx:xx:xx:xx:xx:xx).	mac-address	Not Specified	00:00:00:00:00:00

config system 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|sdwan|...]
    set interface {string}
    set server-select-method [least-rtt|failover]
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
    set log [disable|error|...]
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 protocols.	option	-	cleartext
	Option	Description		
	<i>cleartext</i>	Cleartext DNS over port 53.		
	<i>dot</i>	DNS over TLS.		
	<i>doh</i>	DNS over HTTPS.		
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	
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 .	integer	Minimum value: 1 Maximum value: 10	5
retry	Number of times to retry .	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

Parameter	Description	Type	Size	Default
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
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
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	
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.		

config system ddns

Configure DDNS.

```
config system ddns
  Description: Configure DDNS.
  edit <ddnsid>
    set ddns-server [dyndns.org|dns.net|...]
    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 {user}
    set ddns-domain {string}
    set ddns-username {string}
    set ddns-sn {string}
    set ddns-password {password}
    set use-public-ip [disable|enable]
    set addr-type [ipv4|ipv6]
    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
ddns-server	Select a DDNS service provider.	option	-	
Option	Description			
<i>dyndns.org</i>	members.dyndns.org and dnsalias.com			
<i>dns.net</i>	www.dns.net			
<i>tzo.com</i>	rh.tzo.com			
<i>vavic.com</i>	Peanut Hull			
<i>dipdns.net</i>	dipdnsserver.dipdns.com			
<i>now.net.cn</i>	ip.todayisp.com			
<i>dhs.org</i>	members.dhs.org			
<i>easydns.com</i>	members.easydns.com			
<i>genericDDNS</i>	Generic DDNS based on RFC2136.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.		
	<i>noip.com</i>	dynupdate.no-ip.com		
server-type	Address type of the DDNS server.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	Use IPv4 addressing.		
	<i>ipv6</i>	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
	Option	Description		
	<i>disable</i>	Disable DDNS authentication.		
	<i>tsig</i>	Enable TSIG authentication based on RFC2845.		
ddns-keyname	DDNS update key name.	string	Maximum length: 64	
ddns-key	DDNS update key (base 64 encoding).	user	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable use of public IP address.		
	<i>enable</i>	Enable use of public IP address.		
addr-type	Address type of interface address in DDNS update.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	Use IPv4 address of the interface.		
	<i>ipv6</i>	Use IPv6 address of the interface.		
update-interval	DDNS update interval .	integer	Minimum value: 60 Maximum value: 2592000	300
clear-text	Enable/disable use of clear text connections.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of clear text connections.		
	<i>enable</i>	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 sflow

Configure sFlow.

```
config system sflow
  Description: Configure sFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

config system sflow

Parameter	Description	Type	Size	Default
collector-ip	IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to .	ipv4-address	Not Specified	0.0.0.0
collector-port	UDP port number used for sending sFlow datagrams .	integer	Minimum value: 0 Maximum value: 65535	6343
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
Option	Description			
<i>auto</i>	Set outgoing interface automatically.			
<i>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	

config system vdom-sflow

Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.

```
config system vdom-sflow
  Description: Configure sFlow per VDOM to add or change the IP address and UDP port that
               FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.
  set vdom-sflow [enable|disable]
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set interface-select-method [auto|sdwan|...]
  set interface {string}
end
```

config system vdom-sflow

Parameter	Description	Type	Size	Default
vdom-sflow	Enable/disable the sFlow configuration for the current VDOM.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable sFlow for this VDOM.		
	<i>disable</i>	Disable sFlow for this VDOM.		
collector-ip	IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to .	ipv4-address	Not Specified	0.0.0.0
collector-port	UDP port number used for sending sFlow datagrams .	integer	Minimum value: 0 Maximum value: 65535	6343
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>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	

config system netflow

Configure NetFlow.

```
config system netflow
  Description: Configure NetFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set active-flow-timeout {integer}
  set inactive-flow-timeout {integer}
  set template-tx-timeout {integer}
  set template-tx-counter {integer}
  set interface-select-method [auto|sdwan|...]
```

```

    set interface {string}
end

```

config system netflow

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified	0.0.0.0
active-flow-timeout	Timeout to report active flows .	integer	Minimum value: 60 Maximum value: 3600	1800
inactive-flow-timeout	Timeout for periodic report of finished flows .	integer	Minimum value: 10 Maximum value: 600	15
template-tx-timeout	Timeout for periodic template flowset transmission .	integer	Minimum value: 60 Maximum value: 86400	1800
template-tx-counter	Counter of flowset records before resending a template flowset record.	integer	Minimum value: 10 Maximum value: 6000	20
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	

config system vdom-netflow

Configure NetFlow per VDOM.

```
config system vdom-netflow
    Description: Configure NetFlow per VDOM.
    set vdom-netflow [enable|disable]
    set collector-ip {ipv4-address}
    set collector-port {integer}
    set source-ip {ipv4-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
end
```

config system vdom-netflow

Parameter	Description	Type	Size	Default
vdom-netflow	Enable/disable NetFlow per VDOM.	option	-	disable
Option		Description		
		enable Enable NetFlow per VDOM.		
		disable Disable NetFlow per VDOM.		
collector-ip	NetFlow collector IP address.	ipv4-address	Not Specified	0.0.0.0
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055
source-ip	Source IP address for communication with the NetFlow agent.	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.		
		sdwan Set outgoing interface by SD-WAN or policy routing rules.		
		specify Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

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|sdwan|...]
  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		
		<i>enable</i> Enable configuring DNS servers for the current VDOM.		
		<i>disable</i> 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 protocols.	option	-	cleartext
	Option	Description		
		<i>cleartext</i> Cleartext DNS over port 53.		
		<i>dot</i> DNS over TLS.		
		<i>doh</i> DNS over HTTPS.		
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									
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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr> <tr> <td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr> <tr> <td><i>specify</i></td><td>Set outgoing interface manually.</td></tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 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										
image-type	Image type.	option	-	png										
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td><i>gif</i></td><td>GIF image.</td></tr><tr><td><i>jpg</i></td><td>JPEG image.</td></tr><tr><td><i>tiff</i></td><td>TIFF image.</td></tr><tr><td><i>png</i></td><td>PNG image.</td></tr></tbody></table>				Option	Description	<i>gif</i>	GIF image.	<i>jpg</i>	JPEG image.	<i>tiff</i>	TIFF image.	<i>png</i>	PNG image.
Option	Description													
<i>gif</i>	GIF image.													
<i>jpg</i>	JPEG image.													
<i>tiff</i>	TIFF image.													
<i>png</i>	PNG image.													
image-base64	Image data.	var-string	Maximum length: 32768											

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								
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-									
	<table><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><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></tbody></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	-									

Parameter	Description	Type	Size	Default
	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	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		
buffer	Message string.	var-string	Maximum length: 32768			
header	Header flag.	option	-			
	Option	Description				
	<i>none</i>	No header type.				
	<i>http</i>	HTTP				
	<i>8bit</i>	8 bit.				
format	Format flag.	option	-			
	Option	Description				
	<i>none</i>	No format type.				
	<i>text</i>	Text format.				
	<i>html</i>	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
Option	Description			
<i>none</i>	No header type.			
<i>http</i>	HTTP			
<i>8bit</i>	8 bit.			
format	Format flag.	option	-	
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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
Option	Description			
<i>none</i>	No header type.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	
	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

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		
buffer	Message string.	var-string	Maximum length: 32768			
header	Header flag.	option	-			
	Option	Description				
	<i>none</i>	No header type.				
	<i>http</i>	HTTP				
	<i>8bit</i>	8 bit.				
format	Format flag.	option	-			
	Option	Description				
	<i>none</i>	No format type.				
	<i>text</i>	Text format.				
	<i>html</i>	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
Option	Description			
<i>none</i>	No header type.			
<i>http</i>	HTTP			
<i>8bit</i>	8 bit.			
format	Format flag.	option	-	
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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
Option	Description			
<i>none</i>	No header type.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	
	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	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		
buffer	Message string.	var-string	Maximum length: 32768			
header	Header flag.	option	-			
	Option	Description				
	<i>none</i>	No header type.				
	<i>http</i>	HTTP				
	<i>8bit</i>	8 bit.				
format	Format flag.	option	-			
	Option	Description				
	<i>none</i>	No format type.				
	<i>text</i>	Text format.				
	<i>html</i>	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
Option	Description			
<i>none</i>	No header type.			
<i>http</i>	HTTP			
<i>8bit</i>	8 bit.			
format	Format flag.	option	-	
Option	Description			
<i>none</i>	No format type.			
<i>text</i>	Text format.			
<i>html</i>	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
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	
Option	Description			
<i>none</i>	No header type.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	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
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	default

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Per-vdom replacement messages.		
	<i>utm</i>	For use with UTM settings in firewall policies.		
	<i>auth</i>	For use with authentication pages in firewall policies.		

config mail

Parameter	Description	Type	Size	Default
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 http

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default
	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
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
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

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
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
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

Parameter	Description	Type	Size	Default
	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
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
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

Parameter	Description	Type	Size	Default
	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
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 sslvpn

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default
	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
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 traffic-quota

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default
	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
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
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

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
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
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

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}
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	

Parameter	Description	Type	Size	Default
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

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}, ...
next
end

```

config system snmp community

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

Parameter	Description	Type	Size	Default
query-v2c-port	SNMP v2c query port .	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 .	integer	Minimum value: 1 Maximum value: 65535	162
trap-v1-rport	SNMP v1 trap remote port .	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 .	integer	Minimum value: 1 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port .	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 bgp- established bgp- backward- transition ha- member-up ha-member- down ent- conf-change av-conserve av-bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open power-supply- failure faz- disconnect wc-ap-up wc- ap-down fswctl- session-up fswctl- session-down load-balance- real-server- down per-cpu- high dhcp ospf-nbr- state-change ospf-virtnbr- state-change **

Parameter	Description	Type	Size	Default
Option	Description			
<i>cpu-high</i>	Send a trap when CPU usage is high.			
<i>mem-low</i>	Send a trap when available memory is low.			
<i>log-full</i>	Send a trap when log disk space becomes low.			
<i>intf-ip</i>	Send a trap when an interface IP address is changed.			
<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.			
<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.			
<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.			
<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.			
<i>ips-signature</i>	Send a trap when IPS detects an attack.			
<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.			
<i>av-virus</i>	Send a trap when AntiVirus finds a virus.			
<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.			
<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.			
<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.			
<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.			
<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.			
<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.			
<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.			
<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.			
<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.			
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).			
<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.			
<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.			
<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>power-supply-failure</i>	Send a trap when a power supply fails.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.		
	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.		
	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.		
	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.		
	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.		
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.		
	<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.		
	<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.		

** Values may differ between models.

config hosts

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default
	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. 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
	Option	Description		
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 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 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
status	Enable/disable this SNMP user.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trap-status	Enable/disable traps for this SNMP user.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trap-lport	SNMPv3 local trap port .	integer	Minimum value: 0 Maximum value: 65535	162

Parameter	Description	Type	Size	Default
trap-port	SNMPv3 trap remote port .	integer	Minimum value: 0 Maximum value: 65535	162
queries	Enable/disable SNMP queries for this user.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535	161
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified	
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified	
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 bgp- established bgp- backward- transition ha- member-up ha-member- down ent- conf-change av-conserve av-bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open power-supply- failure faz- disconnect wc-ap-up wc- ap-down fswctl- session-up fswctl- session-down load-balance- real-server- down per-cpu- high dhcp ospf-nbr- state-change ospf-virtnbr- state-change **

Parameter	Description	Type	Size	Default
Option	Description			
<i>cpu-high</i>	Send a trap when CPU usage is high.			
<i>mem-low</i>	Send a trap when available memory is low.			
<i>log-full</i>	Send a trap when log disk space becomes low.			
<i>intf-ip</i>	Send a trap when an interface IP address is changed.			
<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.			
<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.			
<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.			
<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.			
<i>ips-signature</i>	Send a trap when IPS detects an attack.			
<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.			
<i>av-virus</i>	Send a trap when AntiVirus finds a virus.			
<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.			
<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.			
<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.			
<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.			
<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.			
<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.			
<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.			
<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.			
<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.			
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).			
<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.			
<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.			
<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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>power-supply-failure</i>	Send a trap when a power supply fails.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.		
	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.		
	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.		
	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.		
	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.		
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.		
	<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.		
	<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.		
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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv Proto	Privacy (encryption) protocol.	option	-	aes
	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	

** Values may differ between models.

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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
frequency	Update frequency.	option	-	automatic
	Option	Description		
	<i>every</i>	Time interval.		
	<i>daily</i>	Every day.		
	<i>weekly</i>	Every week.		
	<i>automatic</i>	Update automatically within every one hour period.		
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 tunnelling for the FDN.

```
config system autoupdate tunneling
  Description: Configure web proxy tunnelling 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 tunnelling.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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 session-ttl

Configure global session TTL timers for this FortiGate.

```
config system session-ttl
  Description: Configure global session TTL timers for this FortiGate.
  set default {user}
  config port
    Description: Session TTL port.
    edit <id>
      set protocol {integer}
      set start-port {integer}
      set end-port {integer}
      set timeout {user}
    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
protocol	Protocol .	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	

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}
    next
end
set timezone-option [disable|default|...]
set timezone [01|02|...]
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}
    next
end
set server-type [regular|ipsec]
set ip-mode [range|usrgroup]
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 {user}
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}
    next
end
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
status	Enable/disable this DHCP configuration.	option	-	enable
	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
	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
	Option	Description		
	<i>disable</i>	Disable FortiClient On-Net Status.		
	<i>enable</i>	Enable FortiClient On-Net Status.		
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify
	Option	Description		
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.		
	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.		
	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.		

Parameter	Description	Type	Size	Default
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
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
Option	Description			
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.			
<i>default</i>	Clients are assigned the FortiGate's configured NTP servers.			
<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.			
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	

Parameter	Description	Type	Size	Default																										
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																										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Do not set the client's time zone.</td></tr> <tr> <td><i>default</i></td><td>Clients are assigned the FortiGate's configured time zone.</td></tr> <tr> <td><i>specify</i></td><td>Specify the time zone to be assigned to DHCP clients.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Do not set the client's time zone.	<i>default</i>	Clients are assigned the FortiGate's configured time zone.	<i>specify</i>	Specify the time zone to be assigned to DHCP clients.																		
Option	Description																													
<i>disable</i>	Do not set the client's time zone.																													
<i>default</i>	Clients are assigned the FortiGate's configured time zone.																													
<i>specify</i>	Specify the time zone to be assigned to DHCP clients.																													
timezone	Select the time zone to be assigned to DHCP clients.	option	-	00																										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>01</td><td>(GMT-11:00) Midway Island, Samoa</td></tr> <tr> <td>02</td><td>(GMT-10:00) Hawaii</td></tr> <tr> <td>03</td><td>(GMT-9:00) Alaska</td></tr> <tr> <td>04</td><td>(GMT-8:00) Pacific Time (US & Canada)</td></tr> <tr> <td>05</td><td>(GMT-7:00) Arizona</td></tr> <tr> <td>81</td><td>(GMT-7:00) Baja California Sur, Chihuahua</td></tr> <tr> <td>06</td><td>(GMT-7:00) Mountain Time (US & Canada)</td></tr> <tr> <td>07</td><td>(GMT-6:00) Central America</td></tr> <tr> <td>08</td><td>(GMT-6:00) Central Time (US & Canada)</td></tr> <tr> <td>09</td><td>(GMT-6:00) Mexico City</td></tr> <tr> <td>10</td><td>(GMT-6:00) Saskatchewan</td></tr> <tr> <td>11</td><td>(GMT-5:00) Bogota, Lima, Quito</td></tr> </tbody> </table>					Option	Description	01	(GMT-11:00) Midway Island, Samoa	02	(GMT-10:00) Hawaii	03	(GMT-9:00) Alaska	04	(GMT-8:00) Pacific Time (US & Canada)	05	(GMT-7:00) Arizona	81	(GMT-7:00) Baja California Sur, Chihuahua	06	(GMT-7:00) Mountain Time (US & Canada)	07	(GMT-6:00) Central America	08	(GMT-6:00) Central Time (US & Canada)	09	(GMT-6:00) Mexico City	10	(GMT-6:00) Saskatchewan	11	(GMT-5:00) Bogota, Lima, Quito
Option	Description																													
01	(GMT-11:00) Midway Island, Samoa																													
02	(GMT-10:00) Hawaii																													
03	(GMT-9:00) Alaska																													
04	(GMT-8:00) Pacific Time (US & Canada)																													
05	(GMT-7:00) Arizona																													
81	(GMT-7:00) Baja California Sur, Chihuahua																													
06	(GMT-7:00) Mountain Time (US & Canada)																													
07	(GMT-6:00) Central America																													
08	(GMT-6:00) Central Time (US & Canada)																													
09	(GMT-6:00) Mexico City																													
10	(GMT-6:00) Saskatchewan																													
11	(GMT-5:00) Bogota, Lima, Quito																													

Parameter	Description	Type	Size	Default
Option	Description			
12	(GMT-5:00) Eastern Time (US & Canada)			
13	(GMT-5:00) Indiana (East)			
74	(GMT-4:00) Caracas			
14	(GMT-4:00) Atlantic Time (Canada)			
77	(GMT-4:00) Georgetown			
15	(GMT-4:00) La Paz			
87	(GMT-4:00) Paraguay			
16	(GMT-3:00) Santiago			
17	(GMT-3:30) Newfoundland			
18	(GMT-3:00) Brasilia			
19	(GMT-3:00) Buenos Aires			
20	(GMT-3:00) Nuuk (Greenland)			
75	(GMT-3:00) Uruguay			
21	(GMT-2:00) Mid-Atlantic			
22	(GMT-1:00) Azores			
23	(GMT-1:00) Cape Verde Is.			
24	(GMT) Monrovia			
80	(GMT) Greenwich Mean Time			
79	(GMT) Casablanca			
25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.			
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna			
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague			
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris			
78	(GMT+1:00) Namibia			
29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb			
30	(GMT+1:00) West Central Africa			
31	(GMT+2:00) Athens, Sofia, Vilnius			
32	(GMT+2:00) Bucharest			
33	(GMT+2:00) Cairo			

Parameter	Description	Type	Size	Default
	Option	Description		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	44	(GMT+4:30) Kabul		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepura		
	48	(GMT+5:45) Kathmandu		
	45	(GMT+5:00) Ekaterinburg		
	49	(GMT+6:00) Almaty, Novosibirsk		
	50	(GMT+6:00) Astana, Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		
	58	(GMT+8:00) Perth		
	59	(GMT+8:00) Taipei		

Parameter	Description	Type	Size	Default
	Option	Description		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul		
	62	(GMT+9:30) Adelaide		
	63	(GMT+9:30) Darwin		
	61	(GMT+9:00) Yakutsk		
	64	(GMT+10:00) Brisbane		
	65	(GMT+10:00) Canberra, Melbourne, Sydney		
	66	(GMT+10:00) Guam, Port Moresby		
	67	(GMT+10:00) Hobart		
	68	(GMT+10:00) Vladivostok		
	69	(GMT+10:00) Magadan		
	70	(GMT+11:00) Solomon Is., New Caledonia		
	71	(GMT+12:00) Auckland, Wellington		
	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.		
	00	(GMT+12:00) Eniwetok, Kwajalein		
	82	(GMT+12:45) Chatham Islands		
	73	(GMT+13:00) Nuku'alofa		
	86	(GMT+13:00) Samoa		
	76	(GMT+14:00) Kiritimati		
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
	Option	Description		
	regular	Regular DHCP service.		
	ipsec	DHCP over IPsec service.		
ip-mode	Method used to assign client IP.	option	-	range

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>range</i>	Use range defined by start-ip/end-ip to assign client IP.		
	<i>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
	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
	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

Parameter	Description	Type	Size	Default
	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	
ddns-key	DDNS update key (base 64 encoding).	user	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	

config ip-range

Parameter	Description	Type	Size	Default
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

config options

Parameter	Description	Type	Size	Default
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0
type	DHCP option type.	option	-	hex
Option		Description		
		hex DHCP option in hex.		
		string DHCP option in string.		
		ip DHCP option in IP.		
		fqdn DHCP option in domain search option format.		
value	DHCP option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

config exclude-range

Parameter	Description	Type	Size	Default
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

config reserved-address

Parameter	Description	Type	Size	Default
type	DHCP reserved-address type.	option	-	mac

Parameter	Description	Type	Size	Default
	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
	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 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
status	Enable/disable this DHCPv6 configuration.	option	-	enable
Parameter	Description	Option	Size	Default
status	Enable/disable this DHCPv6 configuration.	enable	-	enable
status	Disable this DHCPv6 configuration.	disable	-	enable
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-	disable

Parameter	Description	Type	Size	Default
	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 FortiGate's configured DNS servers.		
	<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.		
dns-search-list	DNS search list options.	option	-	specify
	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	

Parameter	Description	Type	Size	Default
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	
ip-mode	Method used to assign client IP.	option	-	range
Option	Description			
<i>range</i>	Use range defined by start IP/end IP to assign client IP.			
<i>delegated</i>	Use delegated prefix method to assign client IP.			
prefix-mode	Assigning a prefix from a DHCPv6 client or RA.	option	-	dhcp6
Option	Description			
<i>dhcp6</i>	Use delegated prefix from a DHCPv6 client.			
<i>ra</i>	Use prefix from RA.			

config prefix-range

Parameter	Description	Type	Size	Default
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
start-ip	Start of IP range.	ipv6-address	Not Specified	::
end-ip	End of IP range.	ipv6-address	Not Specified	::

config system modem



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61F. It is not available for FortiGate VM64.

Configure MODEM.

```
config system modem
  Description: Configure MODEM.
  set status {enable|disable}
  set pin-init {string}
  set network-init {string}
  set lockdown-lac {string}
  set mode {standalone|redundant}
  set auto-dial {enable|disable}
  set dial-on-demand {enable|disable}
  set idle-timer {integer}
  set redial {none|1|...}
  set reset {integer}
  set holddown-timer {integer}
  set connect-timeout {integer}
  set interface {string}
  set wireless-port {integer}
  set dont-send-CR1 {enable|disable}
  set phone1 {string}
  set dial-cmd1 {string}
  set username1 {string}
  set passwd1 {password}
  set extra-init1 {string}
  set peer-modem1 [generic|actiontec|...]
  set ppp-echo-request1 {enable|disable}
  set authtype1 {option1}, {option2}, ...
  set dont-send-CR2 {enable|disable}
  set phone2 {string}
  set dial-cmd2 {string}
  set username2 {string}
  set passwd2 {password}
  set extra-init2 {string}
  set peer-modem2 [generic|actiontec|...]
  set ppp-echo-request2 {enable|disable}
  set authtype2 {option1}, {option2}, ...
  set dont-send-CR3 {enable|disable}
  set phone3 {string}
  set dial-cmd3 {string}
  set username3 {string}
  set passwd3 {password}
  set extra-init3 {string}
  set peer-modem3 [generic|actiontec|...]
  set ppp-echo-request3 {enable|disable}
  set altmode {enable|disable}
  set authtype3 {option1}, {option2}, ...
  set traffic-check {enable|disable}
  set action {dial|stop|...}
  set distance {integer}
```

```
    set priority {integer}
end
```

config system modem

Parameter	Description	Type	Size	Default
status	Enable/disable Modem support (equivalent to bringing an interface up or down).	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
pin-init	AT command to set the PIN (AT+PIN=<pin>).	string	Maximum length: 127	
network-init	AT command to set the Network name/type (AT+COPS=<mode>,[<format>,<oper>[,<AcT>]]).	string	Maximum length: 127	
lockdown-lac	Allow connection only to the specified Location Area Code (LAC).	string	Maximum length: 127	
mode	Set MODEM operation mode to redundant or standalone.	option	-	standalone
Option		Description		
		<i>standalone</i> Standalone.		
		<i>redundant</i> Redundant for an interface.		
auto-dial	Enable/disable auto-dial after a reboot or disconnection.	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
dial-on-demand	Enable/disable to dial the modem when packets are routed to the modem interface.	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		

Parameter	Description	Type	Size	Default
idle-timer	MODEM connection idle time .	integer	Minimum value: 1 Maximum value: 9999	5
redial	Redial limit .	option	-	none
Option		Description		
<i>none</i>		Forever.		
1		One attempt.		
2		Two attempts.		
3		Three attempts.		
4		Four attempts.		
5		Five attempts.		
6		Six attempts.		
7		Seven attempts.		
8		Eight attempts.		
9		Nine attempts.		
10		Ten attempts.		
reset	Number of dial attempts before resetting modem (0 = never reset).	integer	Minimum value: 0 Maximum value: 10	0
holddown-timer	Hold down timer in seconds .	integer	Minimum value: 1 Maximum value: 60	60
connect-timeout	Connection completion timeout .	integer	Minimum value: 30 Maximum value: 255	90
interface	Name of redundant interface.	string	Maximum length: 63	
wireless-port	Enter wireless port number, 0 for default, 1 for first port, ...	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
dont-send-CR1	Do not send CR when connected (ISP1).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
phone1	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
dial-cmd1	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63	
username1	User name to access the specified dialup account.	string	Maximum length: 63	
passwd1	Password to access the specified dialup account.	password	Not Specified	
extra-init1	Extra initialization string to ISP 1.	string	Maximum length: 127	
peer-modem1	Specify peer MODEM type for phone1.	option	-	generic
	Option	Description		
	<i>generic</i>	All other modem type.		
	<i>actiontec</i>	ActionTec modem.		
	<i>ascend_TNT</i>	Ascend TNT modem.		
ppp-echo-request1	Enable/disable PPP echo-request to ISP 1.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
authtype1	Allowed authentication types for ISP 1.	option	-	pap chap mschap mschapv2
	Option	Description		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
dont-send-CR2	Do not send CR when connected (ISP2).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
phone2	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
dial-cmd2	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63	
username2	User name to access the specified dialup account.	string	Maximum length: 63	
passwd2	Password to access the specified dialup account.	password	Not Specified	
extra-init2	Extra initialization string to ISP 2.	string	Maximum length: 127	
peer-modem2	Specify peer MODEM type for phone2.	option	-	generic
	Option	Description		
	<i>generic</i>	All other modem type.		
	<i>actiontec</i>	ActionTec modem.		
	<i>ascend_TNT</i>	Ascend TNT modem.		
ppp-echo-request2	Enable/disable PPP echo-request to ISP 2.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
authtype2	Allowed authentication types for ISP 2.	option	-	pap chap mschap mschapv2

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
dont-send-CR3	Do not send CR when connected (ISP3).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
phone3	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
dial-cmd3	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63	
username3	User name to access the specified dialup account.	string	Maximum length: 63	
passwd3	Password to access the specified dialup account.	password	Not Specified	
extra-init3	Extra initialization string to ISP 3.	string	Maximum length: 127	
peer-modem3	Specify peer MODEM type for phone3.	option	-	generic
	Option	Description		
	<i>generic</i>	All other modem type.		
	<i>actiontec</i>	ActionTec modem.		
	<i>ascend_TNT</i>	Ascend TNT modem.		
ppp-echo-request3	Enable/disable PPP echo-request to ISP 3.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
altmode	Enable/disable altmode for installations using PPP in China.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
authtype3	Allowed authentication types for ISP 3.	option	-	pap chap mschap mschapv2
	Option	Description		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
traffic-check	Enable/disable traffic-check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Dial up/stop MODEM.	option	-	stop
	Option	Description		
	<i>dial</i>	Dial up number.		
	<i>stop</i>	Stop dialup.		
	<i>none</i>	No action.		
distance	Distance of learned routes .	integer	Minimum value: 1 Maximum value: 255	1
priority	Priority of learned routes .	integer	Minimum value: 0 Maximum value: 4294967295	0

config system 3g-modem custom



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61F. It is not available for FortiGate VM64.

3G MODEM custom.

```
config system 3g-modem custom
  Description: 3G MODEM custom.
  edit <id>
    set vendor {string}
    set model {string}
    set vendor-id {user}
    set product-id {user}
    set class-id {user}
    set init-string {string}
    set modeswitch-string {string}
  next
end
```

config system 3g-modem custom

Parameter	Description	Type	Size	Default
vendor	MODEM vendor name.	string	Maximum length: 35	
model	MODEM model name.	string	Maximum length: 35	
vendor-id	USB vendor ID in hexadecimal format (0000-ffff).	user	Not Specified	
product-id	USB product ID in hexadecimal format (0000-ffff).	user	Not Specified	
class-id	USB interface class in hexadecimal format (00-ff).	user	Not Specified	
init-string	Init string in hexadecimal format (even length).	string	Maximum length: 127	
modeswitch-string	USB modeswitch arguments. e.g: '-v 1410 -p 9030 -V 1410 -P 9032 -u 3'	string	Maximum length: 127	

config system status

System status.

```
config system status
  Description: System status.
end
```

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 .	string	Maximum length: -1	

config system performance firewall packet-distribution

Show distribution statistics.

```
config system performance firewall packet-distribution
    Description: Show distribution statistics.
end
```

config system performance firewall statistics

Show traffic stats.

```
config system performance firewall statistics
    Description: Show traffic stats.
end
```

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 cmdb

System CMDB information.

```
config system cmdb
    Description: System CMDB information.
end
```

config system fortiguard-service

Configuration of FortiGuard services.

```
config system fortiguard-service
    Description: Configuration of FortiGuard services.
end
```

config system fortianalyzer-connectivity

FortiAnalyzer Connectivity.

```
config system fortianalyzer-connectivity
    Description: FortiAnalyzer Connectivity.
end
```

config system checksum status

System checksum.

```
config system checksum status
    Description: System checksum.
end
```

config system mgmt-csum

System checksum for FortiManager use only.

```
config system mgmt-csum
    Description: System checksum for FortiManager use only.
end
```

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 fortiguard-log-service

Configuration of FortiCloud log service.

```
config system fortiguard-log-service
    Description: Configuration of FortiCloud log service.
end
```

config system central-mgmt

Configuration of Central Management Service.

```
config system central-mgmt
    Description: Configuration of Central Management Service.
end
```

config system alias

Configure alias command.

```
config system alias
    Description: Configure alias command.
    edit <name>
        set command {var-string}
    next
end
```

config system alias

Parameter	Description	Type	Size	Default
command	Command list to execute.	var-string	Maximum length: 255	

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 output-size {integer}
set timeout {integer}
next
end

```

config system auto-script

Parameter	Description	Type	Size	Default
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1
start	Script starting mode.	option	-	manual
	Option	Description		
	<i>manual</i>	Starting manually.		
	<i>auto</i>	Starting automatically.		
script	List of FortiOS CLI commands to repeat.	var-string	Maximum length: 1023	
output-size	Number of megabytes to limit script output to .	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 info admin status

Show logged in administrators.

```

config system info admin status
    Description: Show logged in administrators.
end

```

config system info admin ssh

Show SSH status.

```
config system info admin ssh
    Description: Show SSH status.
end
```

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.		

Parameter	Description	Type	Size	Default
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.		
	<i>disable</i>	Disable restriction of authorized manager only.		
serial-number	Serial number.	user	Not Specified	

config system fortimanager

Configure FortiManager.

```
config system fortimanager
  Description: Configure FortiManager.
  set ip {ipv4-address-any}
  set vdom {string}
  set ipsec [enable|disable]
  set central-management [enable|disable]
  set central-mgmt-auto-backup [enable|disable]
  set central-mgmt-schedule-config-restore [enable|disable]
  set central-mgmt-schedule-script-restore [enable|disable]
end
```

config system fortimanager

Parameter	Description	Type	Size	Default
ip	IP address.	ipv4-address-any	Not Specified	0.0.0.0
vdom	Virtual domain name.	string	Maximum length: 31	root
ipsec	Enable/disable FortiManager IPsec tunnel.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiManager IPsec tunnel.		
	<i>disable</i>	Disable FortiManager IPsec tunnel.		
central-management	Enable/disable FortiManager central management.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable central management.		
	<i>disable</i>	Disable central management.		
central-mgmt-auto-backup	Enable/disable central management auto backup.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable auto backup.		
	<i>disable</i>	Disable auto backup.		
central-mgmt-schedule-config-restore	Enable/disable central management schedule config restore.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable central management scheduled restore.		
	<i>disable</i>	Disable central management scheduled restore.		
central-mgmt-schedule-script-restore	Enable/disable central management schedule script restore.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable central management scheduled restore.		
	<i>disable</i>	Disable central management scheduled restore.		

config system fm

Configure FM.

```
config system fm
    Description: Configure FM.
    set status [enable|disable]
    set id {string}
    set ip {ipv4-address}
    set vdom {string}
    set auto-backup [enable|disable]
    set scheduled-config-restore [enable|disable]
    set ipsec [enable|disable]
end
```

config system fm

Parameter	Description	Type	Size	Default
status	Enable/disable FM.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FM.		
	<i>disable</i>	Disable FM.		
id	ID.	string	Maximum length: 35	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
vdom	VDOM.	string	Maximum length: 31	root
auto-backup	Enable/disable automatic backup.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic backup.		
	<i>disable</i>	Disable automatic backup.		
scheduled-config-restore	Enable/disable scheduled configuration restore.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable scheduled configuration restore.		
	<i>disable</i>	Disable scheduled configuration restore.		
ipsec	Enable/disable IPsec.	option	-	disable

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

config system central-management

Configure central management.

```
config system central-management
    Description: Configure central management.
    set mode [normal|backup]
    set type [fortimanager|fortiguard|...]
    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 FortiGate 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|sdwan|...]
    set interface {string}
end
```

config system central-management

Parameter	Description	Type	Size	Default
mode	Central management mode.	option	-	normal

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>normal</i>	Manage and configure this FortiGate from FortiManager.		
	<i>backup</i>	Manage and configure this FortiGate locally and back up its configuration to FortiManager.		
type	Central management type.	option	-	none
	Option	Description		
	<i>fortimanager</i>	FortiManager.		
	<i>fortiguard</i>	Central management of this FortiGate using FortiCloud.		
	<i>none</i>	No central management.		
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiGate.	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 FortiGate.	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 FortiGate.	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 FortiGate.	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 FortiGate from the central management server.	option	-	enable
	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 FortiGate	option	-	enable
	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 FortiGate uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0
fmg-source-ip6	IPv6 source address that this FortiGate uses when communicating with FortiManager.	ipv6-address	Not Specified	::
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
fmgr-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-	8890
	Option	Description		
	<i>8890</i>	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.		
	<i>443</i>	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable inclusion of public FortiGuard servers in the override server list.		
	<i>disable</i>	Disable inclusion of public FortiGuard servers in the override server list.		
enc-algorithm	Encryption strength for communications between the FortiGate and central management.	option	-	high
	Option	Description		
	<i>default</i>	High strength algorithms and medium-strength 128-bit key length algorithms.		
	<i>high</i>	128-bit and larger key length algorithms.		
	<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions.		
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	

config server-list

Parameter	Description	Type	Size	Default
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.		
addr-type	Indicate whether the FortiGate communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 address.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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 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 intrazone [allow|deny]
    set interface <interface-name1>, <interface-name2>, ...
  next
end
```

config system zone

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
intrazone	Allow or deny traffic routing between different interfaces in the same zone .	option	-	deny

Parameter	Description	Type	Size	Default
	Option	Description		
	<ul style="list-style-type: none"> <i>allow</i> Allow traffic between interfaces in the zone. <i>deny</i> Deny traffic between interfaces in the zone. 			
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
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

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
name	Country name.	string	Maximum length: 63	

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 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 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>
        config ip
            Description: Configure IP configuration.
            edit <name>
                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}
set compartment-id {string}
set oci-region {string}
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
        set gcp-project {string}
        set service-account {string}
        set private-key {user}
        set secret-token {user}
        set domain {string}
        set group-name {string}
        set api-key {password}
        set compute-generation {integer}
        set ibm-region [us-south|us-east|...]
        set update-interval {integer}
    next
end

```

config system sdn-connector

Parameter	Description	Type	Size	Default
status	Enable/disable connection to the remote SDN connector.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable connection to this SDN Connector.		
	<i>enable</i>	Enable connection to this SDN Connector.		
type	Type of SDN connector.	option	-	aws
	Option	Description		
	<i>aci</i>	Application Centric Infrastructure (ACI).		
	<i>alicloud</i>	AliCloud Service (ACS).		
	<i>aws</i>	Amazon Web Services (AWS).		
	<i>azure</i>	Microsoft Azure.		
	<i>gcp</i>	Google Cloud Platform (GCP).		
	<i>nsx</i>	VMware NSX.		
	<i>nuage</i>	Nuage VSP.		
	<i>oci</i>	Oracle Cloud Infrastructure.		
	<i>openstack</i>	OpenStack.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>kubernetes</i>	Kubernetes.		
	<i>vmware</i>	VMware vSphere (vCenter & ESXi).		
	<i>sepm</i>	Symantec Endpoint Protection Manager.		
	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).		
	<i>ibm</i>	IBM Cloud Infrastructure.		
	<i>nutanix</i>	Nutanix Prism Central.		
use-metadata-iam	Enable/disable use of IAM role from metadata to call API.	option	-	disable
	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 FortiGate HA service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use for FortiGate HA service.		
	<i>enable</i>	Enable use for FortiGate HA service.		
verify-certificate	Enable/disable server certificate verification.	option	-	enable
	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	
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	

Parameter	Description	Type	Size	Default
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	
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	
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
Option	Description			
<i>global</i>	Global Azure Server.			
<i>china</i>	China Azure Server.			
<i>germany</i>	Germany Azure Server.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>usgov</i>	US Government Azure Server.		
	<i>local</i>	Azure Stack Local Server.		
user-id	User ID.	string	Maximum length: 127	
compartment-id	Compartment ID.	string	Maximum length: 127	
oci-region	OCI server region.	string	Maximum length: 31	
oci-region-type	OCI region type.	option	-	commercial
	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	
gcp-project	GCP project name.	string	Maximum length: 127	
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	Group name of computers.	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

Parameter	Description	Type	Size	Default
ibm-region	IBM cloud region name.	option	-	us-south
Option	Description			
<i>us-south</i>	US South (Dallas) Server.			
<i>us-east</i>	US East (Washington DC) Server.			
<i>germany</i>	Germany (Frankfurt) Server.			
<i>great-britain</i>	Great Britain (London) Server.			
<i>japan</i>	Japan (Tokyo) Server. (GEN1 support only)			
<i>australia</i>	Australia (Sydney) Server. (GEN1 support only)			
update-interval	Dynamic object update interval .	integer	Minimum value: 0 Maximum value: 3600	60

config ip

Parameter	Description	Type	Size	Default
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
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
next-hop	Next hop address.	string	Maximum length: 127	

config route

Parameter	Description	Type	Size	Default
next-hop	Next hop address.	string	Maximum length: 127	

config system ipv6-tunnel

Configure IPv6/IPv4 in IPv6 tunnel.

```
config system ipv6-tunnel
    Description: Configure IPv6/IPv4 in IPv6 tunnel.
    edit <name>
        set source {ipv6-address}
        set destination {ipv6-address}
        set interface {string}
        set use-sdwan [disable|enable]
        set auto-asic-offload [enable|disable]
    next
end
```

config system ipv6-tunnel

Parameter	Description	Type	Size	Default
source	Local IPv6 address of the tunnel.	ipv6-address	Not Specified	::
destination	Remote IPv6 address of the tunnel.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
Option	Description			
<i>disable</i>	Disable use of SD-WAN to reach remote gateway.			
<i>enable</i>	Enable use of SD-WAN to reach remote gateway.			
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
Option	Description			
<i>enable</i>	Enable auto ASIC offloading.			
<i>disable</i>	Disable ASIC offloading.			

* This parameter may not exist in some models.

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|address|...]
    set category {integer}
    set username {string}
    set password {password}
    set comments {var-string}
    set resource {string}
    set user-agent {string}
    set refresh-rate {integer}
    set source-ip {ipv4-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
  next
end
```

config system external-resource

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
status	Enable/disable user resource.	option	-	enable
Option		Description		
		<i>enable</i> Enable user resource.		
		<i>disable</i> Disable user resource.		
type	User resource type.	option	-	category
Option		Description		
		<i>category</i> FortiGuard category.		
		<i>address</i> Firewall IP address.		
		<i>domain</i> Domain Name.		
		<i>malware</i> Malware hash.		

Parameter	Description	Type	Size	Default
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	URI of external resource.	string	Maximum length: 511	
user-agent	HTTP User-Agent header .	string	Maximum length: 127	curl/7.58.0
refresh-rate	Time interval to refresh external resource .	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
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	

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
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable
Option		Description		
		enable Enable this DNS server for IPS URL filter DNS queries.		
		disable Disable this DNS server for IPS URL filter DNS queries.		
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable
Option		Description		
		enable Enable setting.		
		disable 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
status	Enable/disable this server for IPv6 DNS queries.	option	-	enable
Option		Description		
		enable Enable setting.		
		disable Disable setting.		

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
	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
	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
	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 .	integer	Minimum value: 60 Maximum value: 86400	86400
hostname-limit	Limit of the number of hostname table entries .	integer	Minimum value: 0 Maximum value: 50000	5000

Parameter	Description	Type	Size	Default
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 sdwan

Configure redundant Internet connections with multiple outbound links and health-check profiles.

```

config system sdwan
    Description: Configure redundant Internet connections with multiple outbound links and
                 health-check profiles.
    set status [disable|enable]
    set load-balance-mode [source-ip-based|weight-based|...]
    set speedtest-bypass-routing [disable|enable]
    set duplication-max-num {integer}
    set neighbor-hold-down [enable|disable]
    set neighbor-hold-down-time {integer}
    set neighbor-hold-boot-time {integer}
    set fail-detect [enable|disable]
    set fail-alert-interfaces <name1>, <name2>, ...
    config zone
        Description: Configure SD-WAN zones.
        edit <name>
            set service-sla-tie-break [cfg-order|fib-best-match]
        next
    end
    config members
        Description: FortiGate interfaces added to the SD-WAN.
        edit <seq-num>
            set interface {string}
            set zone {string}
            set gateway {ipv4-address}
            set source {ipv4-address}
            set gateway6 {ipv6-address}
            set source6 {ipv6-address}
            set cost {integer}
            set weight {integer}
            set priority {integer}
            set priority6 {integer}
            set spillover-threshold {integer}
            set ingress-spillover-threshold {integer}
            set volume-ratio {integer}
            set status [disable|enable]
            set comment {var-string}
        next
    end
    config health-check

```

Description: SD-WAN status checking or health checking. Identify a server on the Internet and determine how SD-WAN verifies that the FortiGate can communicate with it.

```

edit <name>
    set probe-packets [disable|enable]
    set addr-mode [ipv4|ipv6]
    set system-dns [disable|enable]
    set server {string}
    set detect-mode [active|passive|...]
    set protocol [ping|tcp-echo|...]
    set port {integer}
    set quality-measured-method [half-open|half-close]
    set security-mode [none|authentication]
    set user {string}
    set password {password}
    set packet-size {integer}
    set ha-priority {integer}
    set ftp-mode [passive|port]
    set ftp-file {string}
    set http-get {string}
    set http-agent {string}
    set http-match {string}
    set dns-request-domain {string}
    set dns-match-ip {ipv4-address}
    set interval {integer}
    set probe-timeout {integer}
    set failtime {integer}
    set recoverytime {integer}
    set probe-count {integer}
    set diffservcode {user}
    set update-cascade-interface [enable|disable]
    set update-static-route [enable|disable]
    set sla-fail-log-period {integer}
    set sla-pass-log-period {integer}
    set threshold-warning-packetloss {integer}
    set threshold-alert-packetloss {integer}
    set threshold-warning-latency {integer}
    set threshold-alert-latency {integer}
    set threshold-warning-jitter {integer}
    set threshold-alert-jitter {integer}
    set members <seq-num1>, <seq-num2>, ...
config sla
    Description: Service level agreement (SLA).
    edit <id>
        set link-cost-factor {option1}, {option2}, ...
        set latency-threshold {integer}
        set jitter-threshold {integer}
        set packetloss-threshold {integer}
    next
end
next
end
config neighbor
    Description: Create SD-WAN neighbor from BGP neighbor table to control route
                advertisements according to SLA status.
    edit <ip>
        set member {integer}
        set mode [sla|speedtest]

```

```

        set role [standalone|primary|...]
        set health-check {string}
        set sla-id {integer}
    next
end
config service
    Description: Create SD-WAN rules (also called services) to control how sessions are
        distributed to interfaces in the SD-WAN.
    edit <id>
        set name {string}
        set addr-mode [ipv4|ipv6]
        set input-device <name1>, <name2>, ...
        set input-device-negate [enable|disable]
        set mode [auto|manual|...]
        set minimum-sla-meet-members {integer}
        set hash-mode [round-robin|source-ip-based|...]
        set role [standalone|primary|...]
        set standalone-action [enable|disable]
        set quality-link {integer}
        set tos {user}
        set tos-mask {user}
        set protocol {integer}
        set start-port {integer}
        set end-port {integer}
        set route-tag {integer}
        set dst <name1>, <name2>, ...
        set dst-negate [enable|disable]
        set src <name1>, <name2>, ...
        set dst6 <name1>, <name2>, ...
        set src6 <name1>, <name2>, ...
        set src-negate [enable|disable]
        set users <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set internet-service [enable|disable]
        set internet-service-custom <name1>, <name2>, ...
        set internet-service-custom-group <name1>, <name2>, ...
        set internet-service-name <name1>, <name2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-app-ctrl <id1>, <id2>, ...
        set internet-service-app-ctrl-group <name1>, <name2>, ...
        set health-check <name1>, <name2>, ...
        set link-cost-factor [latency|jitter|...]
        set packet-loss-weight {integer}
        set latency-weight {integer}
        set jitter-weight {integer}
        set bandwidth-weight {integer}
        set link-cost-threshold {integer}
        set hold-down-time {integer}
        set dscp-forward [enable|disable]
        set dscp-reverse [enable|disable]
        set dscp-forward-tag {user}
        set dscp-reverse-tag {user}
    config sla
        Description: Service level agreement (SLA).
        edit <health-check>
            set id {integer}
    next

```

```

        end
        set priority-members <seq-num1>, <seq-num2>, ...
        set priority-zone <name1>, <name2>, ...
        set status [enable|disable]
        set gateway [enable|disable]
        set default [enable|disable]
        set sla-compare-method [order|number]
        set tie-break [zone|cfg-order|...]
        set use-shortcut-sla [enable|disable]
    next
end
config duplication
    Description: Create SD-WAN duplication rule.
    edit <id>
        set service-id <id1>, <id2>, ...
        set srcaddr <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set srcintf <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set service <name1>, <name2>, ...
        set packet-duplication [disable|force|...]
        set packet-de-duplication [enable|disable]
    next
end

```

config system sdwan

Parameter	Description	Type	Size	Default
status	Enable/disable SD-WAN.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SD-WAN.		
	<i>enable</i>	Enable SD-WAN.		
load-balance-mode	Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.	option	-	source-ip-based
	Option	Description		
	<i>source-ip-based</i>	Source IP load balancing. All traffic from a source IP is sent to the same interface.		
	<i>weight-based</i>	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>usage-based</i>	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.		
	<i>source-dest-ip-based</i>	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.		
	<i>measured-volume-based</i>	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.		
speedtest-bypass-routing	Enable/disable bypass routing when speedtest on a SD-WAN member.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SD-WAN.		
	<i>enable</i>	Enable SD-WAN.		
duplication-max-num	Maximum number of interface members a packet is duplicated in the SD-WAN zone .	integer	Minimum value: 2 Maximum value: 4	2
neighbor-hold-down	Enable/disable hold switching from the secondary neighbor to the primary neighbor.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable hold switching from the secondary neighbor to the primary neighbor.		
	<i>disable</i>	Disable hold switching from the secondary neighbor to the primary neighbor.		
neighbor-hold-down-time	Waiting period in seconds when switching from the secondary neighbor to the primary neighbor when hold-down is disabled. .	integer	Minimum value: 0 Maximum value: 10000000	0
neighbor-hold-boot-time	Waiting period in seconds when switching from the primary neighbor to the secondary neighbor from the neighbor start. .	integer	Minimum value: 0 Maximum value: 10000000	0
fail-detect	Enable/disable SD-WAN Internet connection status checking (failure detection).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status checking.		
	<i>disable</i>	Disable status checking.		
fail-alert-interfaces <name>	Physical interfaces that will be alerted. Physical interface name.	string	Maximum length: 79	

config zone

Parameter	Description	Type	Size	Default
service-sla-tie-break	Method of selecting member if more than one meets the SLA.	option	-	cfg-order
	Option	Description		
	<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.		
	<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.		

config members

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	
zone	Zone name.	string	Maximum length: 35	virtual-wan-link
gateway	The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.	ipv4-address	Not Specified	0.0.0.0
source	Source IP address used in the health-check packet to the server.	ipv4-address	Not Specified	0.0.0.0
gateway6	IPv6 gateway.	ipv6-address	Not Specified	::
source6	Source IPv6 address used in the health-check packet to the server.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
cost	Cost of this interface for services in SLA mode .	integer	Minimum value: 0 Maximum value: 4294967295	0
weight	Weight of this interface for weighted load balancing. More traffic is directed to interfaces with higher weights.	integer	Minimum value: 1 Maximum value: 255	1
priority	Priority of the interface for IPv4 . Used for SD-WAN rules or priority rules.	integer	Minimum value: 0 Maximum value: 65535	0
priority6	Priority of the interface for IPv6 . Used for SD-WAN rules or priority rules.	integer	Minimum value: 1 Maximum value: 65535	1024
spillover-threshold	Egress spillover threshold for this interface . When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0
ingress-spillover-threshold	Ingress spillover threshold for this interface . When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0
volume-ratio	Measured volume ratio .	integer	Minimum value: 1 Maximum value: 255	1
status	Enable/disable this interface in the SD-WAN.	option	-	enable
Option	Description			
<i>disable</i>	Disable this interface in the SD-WAN.			
<i>enable</i>	Enable this interface in the SD-WAN.			
comment	Comments.	var-string	Maximum length: 255	

config health-check

Parameter	Description	Type	Size	Default
probe-packets	Enable/disable transmission of probe packets.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable transmission of probe packets.		
	<i>enable</i>	Enable transmission of probe packets.		
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
system-dns	Enable/disable system DNS as the probe server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable system DNS as the probe server.		
	<i>enable</i>	Enable system DNS as the probe server.		
server	IP address or FQDN name of the server.	string	Maximum length: 79	
detect-mode	The mode determining how to detect the server.	option	-	active
	Option	Description		
	<i>active</i>	The probes are sent actively.		
	<i>passive</i>	The traffic measures health without probes.		
	<i>prefer-passive</i>	The probes are sent in case of no new traffic.		
protocol	Protocol used to determine if the FortiGate can communicate with the server.	option	-	ping
	Option	Description		
	<i>ping</i>	Use PING to test the link with the server.		
	<i>tcp-echo</i>	Use TCP echo to test the link with the server.		
	<i>udp-echo</i>	Use UDP echo to test the link with the server.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>http</i>	Use HTTP-GET to test the link with the server.		
	<i>twamp</i>	Use TWAMP to test the link with the server.		
	<i>dns</i>	Use DNS query to test the link with the server.		
	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.		
	<i>ftp</i>	Use FTP to test the link with the server.		
port	Port number used to communicate with the server over the selected protocol .	integer	Minimum value: 0 Maximum value: 65535	0
quality-measured-method	Method to measure the quality of tcp-connect.	option	-	half-open
	Option	Description		
	<i>half-open</i>	Measure the round trip between syn and ack.		
	<i>half-close</i>	Measure the round trip between fin and ack.		
security-mode	Twamp controller security mode.	option	-	none
	Option	Description		
	<i>none</i>	Unauthenticated mode.		
	<i>authentication</i>	Authenticated mode.		
user	The user name to access probe server.	string	Maximum length: 64	
password	Twamp controller password in authentication mode	password	Not Specified	
packet-size	Packet size of a twamp test session,	integer	Minimum value: 64 Maximum value: 1024	64
ha-priority	HA election priority .	integer	Minimum value: 1 Maximum value: 50	1
ftp-mode	FTP mode.	option	-	passive

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>passive</i>	The FTP health-check initiates and establishes the data connection.		
	<i>port</i>	The FTP server initiates and establishes the data connection.		
ftp-file	Full path and file name on the FTP server to download for FTP health-check to probe.	string	Maximum length: 254	
http-get	URL used to communicate with the server if the protocol if the protocol is HTTP.	string	Maximum length: 1024	/
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/
http-match	Response string expected from the server if the protocol is HTTP.	string	Maximum length: 1024	
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255	www.example.com
dns-match-ip	Response IP expected from DNS server if the protocol is DNS.	ipv4-address	Not Specified	0.0.0.0
interval	Status check interval in milliseconds, or the time between attempting to connect to the server .	integer	Minimum value: 500 Maximum value: 3600000	500
probe-timeout	Time to wait before a probe packet is considered lost .	integer	Minimum value: 500 Maximum value: 3600000	500
failtime	Number of failures before server is considered lost .	integer	Minimum value: 1 Maximum value: 3600	5
recoverytime	Number of successful responses received before server is considered recovered .	integer	Minimum value: 1 Maximum value: 3600	5
probe-count	Number of most recent probes that should be used to calculate latency and jitter .	integer	Minimum value: 5 Maximum value: 30	30

Parameter	Description	Type	Size	Default
difffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified	
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable
Option		Description		
		<i>enable</i> Enable update cascade interface.		
		<i>disable</i> Disable update cascade interface.		
update-static-route	Enable/disable updating the static route.	option	-	enable
Option		Description		
		<i>enable</i> Enable updating the static route.		
		<i>disable</i> Disable updating the static route.		
sla-fail-log-period	Time interval in seconds that SLA fail log messages will be generated .	integer	Minimum value: 0 Maximum value: 3600	0
sla-pass-log-period	Time interval in seconds that SLA pass log messages will be generated .	integer	Minimum value: 0 Maximum value: 3600	0
threshold-warning-packetloss	Warning threshold for packet loss .	integer	Minimum value: 0 Maximum value: 100	0
threshold-alert-packetloss	Alert threshold for packet loss .	integer	Minimum value: 0 Maximum value: 100	0
threshold-warning-latency	Warning threshold for latency .	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
threshold-alert-latency	Alert threshold for latency .	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-warning-jitter	Warning threshold for jitter .	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-jitter	Alert threshold for jitter .	integer	Minimum value: 0 Maximum value: 4294967295	0
members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	

config sla

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

config neighbor

Parameter	Description	Type	Size	Default
member	Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
mode	What metric to select the neighbor.	option	-	sla

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sla</i>	Select neighbor based on SLA link quality.		
	<i>speedtest</i>	Select neighbor based on the speedtest status.		
role	Role of neighbor.	option	-	standalone
	Option	Description		
	<i>standalone</i>	Standalone neighbor.		
	<i>primary</i>	Primary neighbor.		
	<i>secondary</i>	Secondary neighbor.		
health-check	SD-WAN health-check name.	string	Maximum length: 35	
sla-id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config service

Parameter	Description	Type	Size	Default
name	SD-WAN rule 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.		
input-device <name>	Source interface name. Interface name.	string	Maximum length: 79	
input-device-negate	Enable/disable negation of input device match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negation of input device match.		
	<i>disable</i>	Disable negation of input device match.		

Parameter	Description	Type	Size	Default
mode	Control how the SD-WAN rule sets the priority of interfaces in the SD-WAN.	option	-	manual
	Option	Description		
	<i>auto</i>	Assign interfaces a priority based on quality.		
	<i>manual</i>	Assign interfaces a priority manually.		
	<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.		
	<i>sla</i>	Assign interfaces a priority based on selected SLA settings.		
	<i>load-balance</i>	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.		
minimum-sla-meet-members	Minimum number of members which meet SLA.	integer	Minimum value: 0 Maximum value: 255	0
hash-mode	Hash algorithm for selected priority members for load balance mode.	option	-	round-robin
	Option	Description		
	<i>round-robin</i>	All traffic are distributed to selected interfaces in equal portions and circular order.		
	<i>source-ip-based</i>	All traffic from a source IP is sent to the same interface.		
	<i>source-dest-ip-based</i>	All traffic from a source IP to a destination IP is sent to the same interface.		
	<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.		
	<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.		
	<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.		
role	Service role to work with neighbor.	option	-	standalone
	Option	Description		
	<i>standalone</i>	Standalone service.		
	<i>primary</i>	Primary service for primary neighbor.		
	<i>secondary</i>	Secondary service for secondary neighbor.		

Parameter	Description	Type	Size	Default
standalone-action	Enable/disable service when selected neighbor role is standalone while service role is not standalone.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable service when selected neighbor role is standalone.		
	<i>disable</i>	Disable service when selected neighbor role is standalone.		
quality-link	Quality grade.	integer	Minimum value: 0 Maximum value: 255	0
tos	Type of service bit pattern.	user	Not Specified	
tos-mask	Type of service evaluated bits.	user	Not Specified	
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535	1
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535	65535
route-tag	IPv4 route map route-tag.	integer	Minimum value: 0 Maximum value: 4294967295	0
dst <name>	Destination address name. Address or address group name.	string	Maximum length: 79	
dst-negate	Enable/disable negation of destination address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable destination address negation.		
	<i>disable</i>	Disable destination address negation.		
src <name>	Source address name. Address or address group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
dst6 <name>	Destination address6 name. Address6 or address6 group name.	string	Maximum length: 79	
src6 <name>	Source address6 name. Address6 or address6 group name.	string	Maximum length: 79	
src-negate	Enable/disable negation of source address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negation.		
	<i>disable</i>	Disable source address negation.		
users <name>	User name. User name.	string	Maximum length: 79	
groups <name>	User groups. Group name.	string	Maximum length: 79	
internet-service	Enable/disable use of Internet service for application-based load balancing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable cloud service to support application-based load balancing.		
	<i>disable</i>	Disable cloud service to support application-based load balancing.		
internet-service-custom <name>	Custom Internet service name list. Custom Internet service name.	string	Maximum length: 79	
internet-service-custom-group <name>	Custom Internet Service group list. Custom Internet Service group name.	string	Maximum length: 79	
internet-service-name <name>	Internet service name list. Internet service name.	string	Maximum length: 79	
internet-service-group <name>	Internet Service group list. Internet Service group name.	string	Maximum length: 79	
internet-service-app-ctrl <id>	Application control based Internet Service ID list. Application control based Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
internet-service-app-ctrl-group <name>	Application control based Internet Service group list. Application control based Internet Service group name.	string	Maximum length: 79	
health-check <name>	Health check list. Health check name.	string	Maximum length: 79	
link-cost-factor	Link cost factor.	option	-	latency
Option		Description		
	<i>latency</i>	Select link based on latency.		
	<i>jitter</i>	Select link based on jitter.		
	<i>packet-loss</i>	Select link based on packet loss.		
	<i>inbandwidth</i>	Select link based on available bandwidth of incoming traffic.		
	<i>outbandwidth</i>	Select link based on available bandwidth of outgoing traffic.		
	<i>bibandwidth</i>	Select link based on available bandwidth of bidirectional traffic.		
	<i>custom-profile-1</i>	Select link based on customized profile.		
packet-loss-weight	Coefficient of packet-loss in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0
latency-weight	Coefficient of latency in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0
jitter-weight	Coefficient of jitter in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0
bandwidth-weight	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0

Parameter	Description	Type	Size	Default						
link-cost-threshold	Percentage threshold change of link cost values that will result in policy route regeneration .	integer	Minimum value: 0 Maximum value: 10000000	10						
hold-down-time	Waiting period in seconds when switching from the back-up member to the primary member .	integer	Minimum value: 0 Maximum value: 10000000	0						
dscp-forward	Enable/disable forward traffic DSCP tag.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable use of forward DSCP tag.</td></tr> <tr> <td><i>disable</i></td><td>Disable use of forward DSCP tag.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of forward DSCP tag.	<i>disable</i>	Disable use of forward DSCP tag.			
Option	Description									
<i>enable</i>	Enable use of forward DSCP tag.									
<i>disable</i>	Disable use of forward DSCP tag.									
dscp-reverse	Enable/disable reverse traffic DSCP tag.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable use of reverse DSCP tag.</td></tr> <tr> <td><i>disable</i></td><td>Disable use of reverse DSCP tag.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable use of reverse DSCP tag.	<i>disable</i>	Disable use of reverse DSCP tag.			
Option	Description									
<i>enable</i>	Enable use of reverse DSCP tag.									
<i>disable</i>	Disable use of reverse DSCP tag.									
dscp-forward-tag	Forward traffic DSCP tag.	user	Not Specified							
dscp-reverse-tag	Reverse traffic DSCP tag.	user	Not Specified							
priority-members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295							
priority-zone <name>	Priority zone name list. Priority zone name.	string	Maximum length: 79							
status	Enable/disable SD-WAN service.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable SD-WAN service.</td></tr> <tr> <td><i>disable</i></td><td>Disable SD-WAN service.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable SD-WAN service.	<i>disable</i>	Disable SD-WAN service.			
Option	Description									
<i>enable</i>	Enable SD-WAN service.									
<i>disable</i>	Disable SD-WAN service.									
gateway	Enable/disable SD-WAN service gateway.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable SD-WAN service gateway.		
	<i>disable</i>	Disable SD-WAN service gateway.		
default	Enable/disable use of SD-WAN as default service.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of SD-WAN as default service.		
	<i>disable</i>	Disable use of SD-WAN as default service.		
sla-compare-method	Method to compare SLA value for SLA mode.	option	-	order
	Option	Description		
	<i>order</i>	Compare SLA value based on the order of health-check.		
	<i>number</i>	Compare SLA value based on the number of satisfied health-check. Limits health-checks to only configured member interfaces.		
tie-break	Method of selecting member if more than one meets the SLA.	option	-	zone
	Option	Description		
	<i>zone</i>	Use the setting that is configured for the members' zone.		
	<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.		
	<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.		
use-shortcut-sla	Enable/disable use of ADVVPN shortcut for quality comparison.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of ADVVPN shortcut for quality comparison.		
	<i>disable</i>	Disable use of ADVVPN shortcut for quality comparison.		

config sla

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

config duplication

Parameter	Description	Type	Size	Default
service-id <id>	SD-WAN service rule ID list. SD-WAN service rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	
srcaddr <name>	Source address or address group names. Address or address group name.	string	Maximum length: 79	
dstaddr <name>	Destination address or address group names. Address or address group name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79	
dstaddr6 <name>	Destination address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79	
srcintf <name>	Incoming (ingress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79	
service <name>	Service and service group name. Service and service group name.	string	Maximum length: 79	
packet-duplication	Configure packet duplication method.	option	-	disable
Option	Description			
<i>disable</i>	Disable packet duplication.			
<i>force</i>	Duplicate packets across all interface members of the SD-WAN zone.			
<i>on-demand</i>	Duplicate packets across all interface members of the SD-WAN zone based on the link quality.			

Parameter	Description	Type	Size	Default
packet-de-duplication	Enable/disable discarding of packets that have been duplicated.	option	-	disable
Option	Description			
<i>enable</i>	Enable discarding of packets that have been duplicated.			
<i>disable</i>	Disable discarding of packets that have been duplicated.			

config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set interface {string}
    set ip-version [4|6]
    set remote-gw6 {ipv6-address}
    set local-gw6 {ipv6-address}
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address-any}
    set use-sdwan [disable|enable]
    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 dscp-copying [disable|enable]
    set diffservcode {user}
    set keepalive-interval {integer}
    set keepalive-failtimes {integer}
  next
end
```

config system gre-tunnel

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 15	
ip-version	IP version to use for VPN interface.	option	-	4
Option	Description			
4	Use IPv4 addressing for gateways.			
6	Use IPv6 addressing for gateways.			

Parameter	Description	Type	Size	Default						
remote-gw6	IPv6 address of the remote gateway.	ipv6-address	Not Specified	::						
local-gw6	IPv6 address of the local gateway.	ipv6-address	Not Specified	::						
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						
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable use of SD-WAN to reach remote gateway.</td></tr> <tr> <td><i>enable</i></td><td>Enable use of SD-WAN to reach remote gateway.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Disable use of SD-WAN to reach remote gateway.	<i>enable</i>	Enable use of SD-WAN to reach remote gateway.
Option	Description									
<i>disable</i>	Disable use of SD-WAN to reach remote gateway.									
<i>enable</i>	Enable use of SD-WAN to reach remote gateway.									
sequence-number-transmission *	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Include sequence numbers in transmitted GRE packets.</td></tr> <tr> <td><i>enable</i></td><td>Do not include sequence numbers in transmitted GRE packets.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Include sequence numbers in transmitted GRE packets.	<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.
Option	Description									
<i>disable</i>	Include sequence numbers in transmitted GRE packets.									
<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.									
sequence-number-reception *	Enable/disable validating sequence numbers in received GRE packets.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Do not validate sequence number in received GRE packets.</td></tr> <tr> <td><i>enable</i></td><td>Validate sequence numbers in received GRE packets.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Do not validate sequence number in received GRE packets.	<i>enable</i>	Validate sequence numbers in received GRE packets.
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						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Do not include checksums in transmitted GRE packets.</td></tr> <tr> <td><i>enable</i></td><td>Include checksums in transmitted GRE packets.</td></tr> </tbody> </table>					Option	Description	<i>disable</i>	Do not include checksums in transmitted GRE packets.	<i>enable</i>	Include checksums in transmitted GRE packets.
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						

Parameter	Description	Type	Size	Default	
	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 .	integer	Minimum value: 0 Maximum value: 4294967295	0	
key-inbound *	Require received GRE packets contain this key .	integer	Minimum value: 0 Maximum value: 4294967295	0	
dscp-copying	Enable/disable DSCP copying.	option	-	disable	
	Option	Description			
	<i>disable</i>	Disable DSCP copying.			
	<i>enable</i>	Enable DSCP copying.			
diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified		
keepalive-interval	Keepalive message interval .	integer	Minimum value: 0 Maximum value: 32767	0	
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down .	integer	Minimum value: 1 Maximum value: 255	10	

* This parameter may not exist in some models.

config system ipsec-aggregate

Configure an aggregate of IPsec tunnels.

```
config system ipsec-aggregate
  Description: Configure an aggregate of IPsec tunnels.
  edit <name>
    set member <tunnel-name1>, <tunnel-name2>, ...
    set algorithm [L3|L4|...]
  next
end
```

config system ipsec-aggregate

Parameter	Description	Type	Size	Default
member <tunnel-name>	Member tunnels of the aggregate. Tunnel name.	string	Maximum length: 79	
algorithm	Frame distribution algorithm.	option	-	round-robin
Option	Description			
<i>L3</i>	Use layer 3 address for distribution.			
<i>L4</i>	Use layer 4 information for distribution.			
<i>round-robin</i>	Per-packet round-robin distribution.			
<i>redundant</i>	Use first tunnel that is up for all traffic.			
<i>weighted-round-robin</i>	Weighted round-robin distribution.			

config system ipip-tunnel

Configure IP in IP Tunneling.

```
config system ipip-tunnel
  Description: Configure IP in IP Tunneling.
  edit <name>
    set interface {string}
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address-any}
    set use-sdwan [disable|enable]
    set auto-asic-offload [enable|disable]
  next
end
```

config system ipip-tunnel

Parameter	Description	Type	Size	Default
interface	Interface name that is associated with the incoming traffic from available options.	string	Maximum length: 15	
remote-gw	IPv4 address for the remote gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	IPv4 address for the local gateway.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
Option	Description			
<i>disable</i>	Disable use of SD-WAN to reach remote gateway.			
<i>enable</i>	Enable use of SD-WAN to reach remote gateway.			
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
Option	Description			
<i>enable</i>	Enable auto ASIC offloading.			
<i>disable</i>	Disable ASIC offloading.			

* This parameter may not exist in some models.

config system mobile-tunnel

Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.

```
config system mobile-tunnel
    Description: Configure Mobile tunnels, an implementation of Network Mobility (NEMO)
                 extensions for Mobile IPv4 RFC5177.
    edit <name>
        set status [disable|enable]
        set roaming-interface {string}
        set home-agent {ipv4-address}
        set home-address {ipv4-address}
        set renew-interval {integer}
        set lifetime {integer}
        set reg-interval {integer}
        set reg-retry {integer}
        set n-mhae-spi {integer}
        set n-mhae-key-type [ascii|base64]
        set n-mhae-key {user}
        set hash-algorithm {option}
        set tunnel-mode {option}
        config network
            Description: NEMO network configuration.
            edit <id>
                set interface {string}
                set prefix {ipv4-classnet}
            next
        end
    next
end
```

config system mobile-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable this mobile tunnel.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this mobile tunnel.		
	<i>enable</i>	Enable this mobile tunnel.		
roaming-interface	Select the associated interface name from available options.	string	Maximum length: 15	
home-agent	IPv4 address of the NEMO HA (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
home-address	Home IP address (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
renew-interval	Time before lifetime expiraton to send NMMO HA re-registration .	integer	Minimum value: 5 Maximum value: 60	60
lifetime	NMMO HA registration request lifetime .	integer	Minimum value: 180 Maximum value: 65535	65535
reg-interval	NMMO HA registration interval .	integer	Minimum value: 5 Maximum value: 300	5
reg-retry	Maximum number of NMMO HA registration retries .	integer	Minimum value: 1 Maximum value: 30	3
n-mhae-spi	NEMO authentication SPI .	integer	Minimum value: 0 Maximum value: 4294967295	256
n-mhae-key-type	NEMO authentication key type (ascii or base64).	option	-	ascii
	Option	Description		
	<i>ascii</i>	The authentication key is an ASCII string.		
	<i>base64</i>	The authentication key is Base64 encoded.		

Parameter	Description	Type	Size	Default
n-mhae-key	NEMO authentication key.	user	Not Specified	
hash-algorithm	Hash Algorithm (Keyed MD5).	option	-	hmac-md5
	Option	Description		
	<i>hmac-md5</i>	Keyed MD5.		
tunnel-mode	NEMO tunnnel mode (GRE tunnel).	option	-	gre
	Option	Description		
	<i>gre</i>	GRE tunnel.		

config network

Parameter	Description	Type	Size	Default
interface	Select the associated interface name from available options.	string	Maximum length: 15	
prefix	Class IP and Netmask with correction (Format:xxx.xxx.xxx.xxx xxx.xxx.xxx or xxx.xxx.xxx.xxx/x).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config system pppoe-interface

Configure the PPPoE interfaces.

```
config system pppoe-interface
  Description: Configure the PPPoE interfaces.
  edit <name>
    set dial-on-demand {enable|disable}
    set ipv6 {enable|disable}
    set device {string}
    set username {string}
    set password {password}
    set auth-type {auto|pap|...}
    set ipunnumbered {ipv4-address}
    set pppoe-unnumbered-negotiate {enable|disable}
    set idle-timeout {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}
  next
end
```

config system pppoe-interface

Parameter	Description	Type	Size	Default
dial-on-demand	Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE interface.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dial on demand.		
	<i>disable</i>	Disable dial on demand.		
ipv6	Enable/disable IPv6 Control Protocol (IPv6CP).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPv6CP.		
	<i>disable</i>	Disable IPv6CP.		
device	Name for the physical interface.	string	Maximum length: 15	
username	User name.	string	Maximum length: 64	
password	Enter the password.	password	Not Specified	
auth-type	PPP authentication type to use.	option	-	auto
	Option	Description		
	<i>auto</i>	Automatically choose the authentication method.		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
ipunnumbered	PPPoE unnumbered IP.	ipv4-address	Not Specified	0.0.0.0
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable PPPoE unnumbered negotiation.		
	<i>disable</i>	Disable PPPoE unnumbered negotiation.		

Parameter	Description	Type	Size	Default
idle-timeout	PPPoE auto disconnect after idle timeout .	integer	Minimum value: 0 Maximum value: 4294967295	0
disc-retry-timeout	PPPoE discovery init timeout value in .	integer	Minimum value: 0 Maximum value: 4294967295	1
padt-retry-timeout	PPPoE terminate timeout value in .	integer	Minimum value: 0 Maximum value: 4294967295	1
service-name	PPPoE service name.	string	Maximum length: 63	
ac-name	PPPoE AC 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

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}
  next
end
```

config system vxlan

Parameter	Description	Type	Size	Default
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 or multicast.	option	-	ipv4-unicast
Option		Description		
<i>ipv4-unicast</i>		Use IPv4 unicast addressing over the VXLAN.		
<i>ipv6-unicast</i>		Use IPv6 unicast addressing over the VXLAN.		
<i>ipv4-multicast</i>		Use IPv4 multicast addressing over the VXLAN.		
<i>ipv6-multicast</i>		Use IPv6 multicast addressing over the VXLAN.		
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 .	integer	Minimum value: 1 Maximum value: 65535	4789
multicast-ttl	VXLAN multicast TTL .	integer	Minimum value: 1 Maximum value: 255	0

config system geneve

Configure GENEVE devices.

```
config system geneve
  Description: Configure GENEVE devices.
  edit <name>
    set interface {string}
```

```

set vni {integer}
set type [ethernet|ppp]
set ip-version [ipv4-unicast|ipv6-unicast]
set remote-ip {ipv4-address}
set remote-ip6 {ipv6-address}
set dstport {integer}
next
end

```

config system geneve

Parameter	Description	Type	Size	Default						
interface	Outgoing interface for GENEVE encapsulated traffic.	string	Maximum length: 15							
vni	GENEVE network ID.	integer	Minimum value: 0 Maximum value: 16777215	0						
type	GENEVE type.	option	-	ethernet						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>ethernet</i></td><td>Internal packet includes Ethernet header.</td></tr> <tr> <td><i>ppp</i></td><td>Internal packet does not include Ethernet header.</td></tr> </tbody> </table>	Option	Description	<i>ethernet</i>	Internal packet includes Ethernet header.	<i>ppp</i>	Internal packet does not include Ethernet header.			
Option	Description									
<i>ethernet</i>	Internal packet includes Ethernet header.									
<i>ppp</i>	Internal packet does not include Ethernet header.									
ip-version	IP version to use for the GENEVE interface and so for communication over the GENEVE. IPv4 or IPv6 unicast.	option	-	ipv4-unicast						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>ipv4-unicast</i></td><td>Use IPv4 unicast addressing over the GENEVE.</td></tr> <tr> <td><i>ipv6-unicast</i></td><td>Use IPv6 unicast addressing over the GENEVE.</td></tr> </tbody> </table>	Option	Description	<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the GENEVE.	<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the GENEVE.			
Option	Description									
<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the GENEVE.									
<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the GENEVE.									
remote-ip	IPv4 address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv4-address	Not Specified	0.0.0.0						
remote-ip6	IPv6 IP address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv6-address	Not Specified	::						
dstport	GENEVE destination port .	integer	Minimum value: 1 Maximum value: 65535	6081						

config system virtual-wire-pair

Configure virtual wire pairs.

```

config system virtual-wire-pair
    Description: Configure virtual wire pairs.
    edit <name>
        set member <interface-name1>, <interface-name2>, ...
        set wildcard-vlan [enable|disable]
        set vlan-filter {user}
    next
end

```

config system virtual-wire-pair

Parameter	Description	Type	Size	Default
member <interface- name>	Interfaces belong to the virtual-wire-pair. Interface name.	string	Maximum length: 79	
wildcard-vlan	Enable/disable wildcard VLAN.	option	-	disable
	Option	Description		
	enable	Enable wildcard VLAN.		
	disable	Disable wildcard VLAN.		
vlan-filter	Set VLAN filters.	user	Not Specified	

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 source-ip {ipv4-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
status	Enable/disable this DNS zone.	option	-	enable
	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
	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
	Option	Description		
	<i>shadow</i>	Shadow DNS zone to serve internal clients.		
	<i>public</i>	Public DNS zone to serve public clients.		
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

Parameter	Description	Type	Size	Default						
contact	Email address of the administrator for this zone. You can specify only the username (e.g. admin) or full email address (e.g. admin@test.com) When using a simple username, the domain of the email will be this zone.	string	Maximum length: 255	host						
ttl	Default time-to-live value for the entries of this DNS zone .	integer	Minimum value: 0 Maximum value: 2147483647	86400						
authoritative	Enable/disable authoritative zone.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable authoritative zone.</td></tr> <tr> <td><i>disable</i></td><td>Disable authoritative zone.</td></tr> </tbody> </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							
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0						
rr-max	Maximum number of resource records .	integer	Minimum value: 10 Maximum value: 65536	16384						

config dns-entry

Parameter	Description	Type	Size	Default								
status	Enable/disable resource record status.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>A</i></td><td>Host type.</td></tr> <tr> <td><i>NS</i></td><td>Name server type.</td></tr> <tr> <td><i>CNAME</i></td><td>Canonical name type.</td></tr> </tbody> </table>	Option	Description	<i>A</i>	Host type.	<i>NS</i>	Name server type.	<i>CNAME</i>	Canonical name type.			
Option	Description											
<i>A</i>	Host type.											
<i>NS</i>	Name server type.											
<i>CNAME</i>	Canonical name type.											

Parameter	Description	Type	Size	Default
	Option	Description		
	MX	Mail exchange type.		
	AAAA	IPv6 host type.		
	PTR	Pointer type.		
	PTR_V6	IPv6 pointer type.		
ttl	Time-to-live for this entry .	integer	Minimum value: 0 Maximum value: 2147483647	0
preference	DNS entry preference, 0 is the highest preference	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]
  next
end
```

config system dns-server

Parameter	Description	Type	Size	Default
mode	DNS server mode.	option	-	recursive
Option		Description		
		recursive Shadow DNS database and forward.		
		non-recursive Public DNS database only.		
		forward-only Forward only.		
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35	
doh	DNS over HTTPS.	option	-	disable
Option		Description		
		enable Enable DNS over HTTPS.		
		disable Disable DNS over HTTPS.		

config system resource-limits

Configure resource limits.

```
config system resource-limits
    Description: Configure resource limits.
    set session {integer}
    set ipsec-phase1 {integer}
    set ipsec-phase2 {integer}
    set ipsec-phase1-interface {integer}
    set ipsec-phase2-interface {integer}
    set dialup-tunnel {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 sslvpn {integer}
    set proxy {integer}
    set log-disk-quota {integer}
end
```

config system resource-limits

Parameter	Description	Type	Size	Default
session	Maximum number of sessions.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1	Maximum number of VPN IPsec phase1 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2	Maximum number of VPN IPsec phase2 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-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	
dialup-tunnel	Maximum number of dial-up 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	
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
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	
sslvpn	Maximum number of SSL-VPN.	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 MiB.	integer	Minimum value: 0 Maximum value: 4294967295 **	

** Values may differ between models.

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 session {user}
    set ipsec-phase1 {user}
    set ipsec-phase2 {user}
    set ipsec-phase1-interface {user}
    set ipsec-phase2-interface {user}
    set dialup-tunnel {user}
    set firewall-policy {user}
    set firewall-address {user}
    set firewall-addrgrp {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 sslvpn {user}
    set proxy {user}
    set log-disk-quota {user}
  next
end
```

config system vdom-property

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
snmp-index	Permanent SNMP Index of the virtual domain .	integer	Minimum value: 1 Maximum value: 2147483647	0
session	Maximum guaranteed number of sessions.	user	Not Specified	
ipsec-phase1	Maximum guaranteed number of VPN IPsec phase 1 tunnels.	user	Not Specified	
ipsec-phase2	Maximum guaranteed number of VPN IPsec phase 2 tunnels.	user	Not Specified	
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	
dialup-tunnel	Maximum guaranteed number of dial-up 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-addrgrp	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	
sslvpn	Maximum guaranteed number of SSL-VPNs.	user	Not Specified	

Parameter	Description	Type	Size	Default
proxy	Maximum guaranteed number of concurrent proxy users.	user		Not Specified
log-disk-quota	Log disk quota in MiB (range depends on how much disk space is available).	user		Not Specified

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}
            next
        end
    next
end
```

config system speed-test-server

Parameter	Description	Type	Size	Default
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	0

config host

Parameter	Description	Type	Size	Default
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

Parameter	Description	Type	Size	Default
user	Speed test host user name.	string	Maximum length: 64	
password	Speed test host password.	password	Not Specified	

config system lldp network-policy

Configure LLDP network policy.

```
config system lldp network-policy
    Description: Configure LLDP network policy.
    edit <name>
        set comment {var-string}
        config voice
            Description: Voice.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config voice-signaling
            Description: Voice signaling.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config guest
            Description: Guest.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config guest-voice-signaling
            Description: Guest Voice Signaling.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config softphone
            Description: Softphone.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
```

```

        end
    config video-conferencing
        Description: Video Conferencing.
        set status {disable|enable}
        set tag {none|dot1q|...}
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
    config streaming-video
        Description: Streaming Video.
        set status {disable|enable}
        set tag {none|dot1q|...}
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
    config video-signaling
        Description: Video Signaling.
        set status {disable|enable}
        set tag {none|dot1q|...}
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
next
end

```

config system lldp network-policy

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	

config voice

Parameter	Description	Type	Size	Default						
status	Enable/disable advertising this policy.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>disable</td> <td>Disable advertising this LLDP network policy.</td> </tr> <tr> <td>enable</td> <td>Enable advertising this LLDP network policy.</td> </tr> </tbody> </table>	Option	Description	disable	Disable advertising this LLDP network policy.	enable	Enable advertising this LLDP network policy.			
Option	Description									
disable	Disable advertising this LLDP network policy.									
enable	Enable advertising this LLDP network policy.									
tag	Advertise tagged or untagged traffic.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>none</td> <td>Advertise that untagged frames should be used.</td> </tr> </tbody> </table>	Option	Description	none	Advertise that untagged frames should be used.					
Option	Description									
none	Advertise that untagged frames should be used.									

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.			
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0	
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5	
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46	

config voice-signaling

Parameter	Description	Type	Size	Default	
status	Enable/disable advertising this policy.	option	-	disable	
	Option	Description			
	<i>disable</i>	Disable advertising this LLDP network policy.			
	<i>enable</i>	Enable advertising this LLDP network policy.			
tag	Advertise tagged or untagged traffic.	option	-	none	
	Option	Description			
	<i>none</i>	Advertise that untagged frames should be used.			
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.			
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0	
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5	

Parameter	Description	Type	Size	Default
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

config guest

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
Parameter	Description	Type	Size	Default
tag	Advertise tagged or untagged traffic.	option	-	none
Parameter	Description	Type	Size	Default
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

config guest-voice-signaling

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	Option	Description		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

config softphone

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	Option	Description		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		

Parameter	Description	Type	Size	Default
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

config video-conferencing

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
Option		Description		
<i>disable</i>		Disable advertising this LLDP network policy.		
<i>enable</i>		Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
Option		Description		
<i>none</i>		Advertise that untagged frames should be used.		
<i>dot1q</i>		Advertise that 802.1Q (VLAN) tagging should be used.		
<i>dot1p</i>		Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

config streaming-video

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	Option	Description		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

config video-signaling

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>none</i>	Advertise that untagged frames should be used.			
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.			
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094	0	
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7	5	
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46	

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 schedules <name1>, <name2>, ...
    set dynamic-server [disable|enable]
    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
status	Enable/disable scheduled speed test.	option	-	enable

Parameter	Description	Type	Size	Default
	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	
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.		
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
update-inbandwidth-minimum	Minimum downloading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0

Parameter	Description	Type	Size	Default
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 standalone-cluster

Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.

```
config system standalone-cluster
  Description: Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.
  set standalone-group-id {integer}
  set group-member-id {integer}
  set layer2-connection [available|unavailable]
  set session-sync-dev {user}
  set encryption [enable|disable]
  set psksecret {password-3}
end
```

config system standalone-cluster

Parameter	Description	Type	Size	Default
standalone-group-id	Cluster group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255	0
group-member-id	Cluster member ID .	integer	Minimum value: 0 Maximum value: 15	0
layer2-connection	Indicate whether layer 2 connections are present among FGSP members.	option	-	unavailable
Option	Description			
<i>available</i>	There exist layer 2 connections among FGSP members.			
<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.			

Parameter	Description	Type	Size	Default
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified	
	Option	Description		
	enable	Enable encryption when synchronizing sessions.		
	disable	Disable encryption when synchronizing sessions.		
psksecret	Pre-shared secret for session synchronization (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	

config system cluster-sync

Configure FortiGate Session Life Support Protocol (FGSP) session synchronization.

```
config system cluster-sync
    Description: Configure FortiGate Session Life Support Protocol (FGSP) session
                 synchronization.
    edit <sync-id>
        set peervd {string}
        set peerip {ipv4-address}
        set syncvd <name1>, <name2>, ...
        set down-intfs-before-sess-sync <name1>, <name2>, ...
        set hb-interval {integer}
        set hb-lost-threshold {integer}
        set ipsec-tunnel-sync [enable|disable]
        set ike-monitor [enable|disable]
        set ike-monitor-interval {integer}
        set ike-heartbeat-interval {integer}
        set secondary-add-ipsec-routes [enable|disable]
        config session-sync-filter
            Description: Add one or more filters if you only want to synchronize some sessions.
                         Use the filter to configure the types of sessions to synchronize.
            set srcintf {string}
            set dstintf {string}
            set srcaddr {ipv4-classnet-any}
            set dstaddr {ipv4-classnet-any}
            set srcaddr6 {ipv6-network}
            set dstaddr6 {ipv6-network}
            config custom-service
                Description: Only sessions using these custom services are synchronized. Use source
                             and destination port ranges to define these custome services.
                edit <id>
                    set src-port-range {user}
                    set dst-port-range {user}
                next
            end
        end
    next
end
```

config system cluster-sync

Parameter	Description	Type	Size	Default						
peervd	VDOM that contains the session synchronization link interface on the peer unit. Usually both peers would have the same peervd.	string	Maximum length: 31	root						
peerip	IP address of the interface on the peer unit that is used for the session synchronization link.	ipv4-address	Not Specified	0.0.0.0						
syncvd <name>	Sessions from these VDOMs are synchronized using this session synchronization configuration. VDOM name.	string	Maximum length: 79							
down-intfs-before-sess-sync <name>	List of interfaces to be turned down before session synchronization is complete. Interface name.	string	Maximum length: 79							
hb-interval	Heartbeat interval .	integer	Minimum value: 1 Maximum value: 10	2						
hb-lost-threshold	Lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 10	3						
ipsec-tunnel-sync	Enable/disable IPsec tunnel synchronization.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable IPsec tunnel synchronization.</td></tr> <tr> <td><i>disable</i></td><td>Disable IPsec tunnel synchronization.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable IPsec tunnel synchronization.	<i>disable</i>	Disable IPsec tunnel synchronization.
Option	Description									
<i>enable</i>	Enable IPsec tunnel synchronization.									
<i>disable</i>	Disable IPsec tunnel synchronization.									
ike-monitor	Enable/disable IKE HA monitor.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable IKE HA monitor.</td></tr> <tr> <td><i>disable</i></td><td>Disable IKE HA monitor.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable IKE HA monitor.	<i>disable</i>	Disable IKE HA monitor.
Option	Description									
<i>enable</i>	Enable IKE HA monitor.									
<i>disable</i>	Disable IKE HA monitor.									
ike-monitor-interval	IKE HA monitor interval .	integer	Minimum value: 10 Maximum value: 300	15						

Parameter	Description	Type	Size	Default
ike-heartbeat-interval	IKE heartbeat interval .	integer	Minimum value: 1 Maximum value: 60	3
	Option	Description		
secondary-add-ipsec-routes	Enable/disable IKE route announcement on the backup unit.	option	-	enable
	enable	Add IKE routes to the backup unit.		
	disable	Do not add IKE routes to the backup unit.		

config session-sync-filter

Parameter	Description	Type	Size	Default
srcintf	Only sessions from this interface are synchronized. You can only enter one interface name. To synchronize sessions for multiple source interfaces, add multiple filters.	string	Maximum length: 15	
dstintf	Only sessions to this interface are synchronized. You can only enter one interface name. To synchronize sessions to multiple destination interfaces, add multiple filters.	string	Maximum length: 15	
srcaddr	Only sessions from this IPv4 address are synchronized. You can only enter one address. To synchronize sessions from multiple source addresses, add multiple filters.	ipv4-classnet-any	Not Specified	0.0.0.0
dstaddr	Only sessions to this IPv4 address are synchronized. You can only enter one address. To synchronize sessions for multiple destination addresses, add multiple filters.	ipv4-classnet-any	Not Specified	0.0.0.0
srcaddr6	Only sessions from this IPv6 address are synchronized. You can only enter one address. To synchronize sessions from multiple source addresses, add multiple filters.	ipv6-network	Not Specified	::/0
dstaddr6	Only sessions to this IPv6 address are synchronized. You can only enter one address. To synchronize sessions for multiple destination addresses, add multiple filters.	ipv6-network	Not Specified	::/0

config custom-service

Parameter	Description	Type	Size	Default
src-port-range	Custom service source port range.	user	Not Specified	0-0
dst-port-range	Custom service destination port range.	user	Not Specified	0-0

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 load-balance-servers {integer}
    set auto-join-forticloud [enable|disable]
    set update-server-location [usa|any]
    set sandbox-region {string}
    set update-ffdb [enable|disable]
    set update-uwdb [enable|disable]
    set update-extdb [enable|disable]
    set update-build-proxy [enable|disable]
    set persistent-connection [enable|disable]
    set antispam-force-off [enable|disable]
    set antispam-cache [enable|disable]
    set antispam-cache-ttl {integer}
    set antispam-cache-mpercent {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-mpercent {integer}
    set outbreak-prevention-license {integer}
    set outbreak-prevention-expiration {integer}
    set outbreak-prevention-timeout {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 {ipv4-address}
set proxy-server-port {integer}
set proxy-username {string}
set proxy-password {password}
set videofilter-license {integer}
set videofilter-expiration {integer}
set ddns-server-ip {ipv4-address}
set ddns-server-ip6 {ipv6-address}
set ddns-server-port {integer}
set interface-select-method [auto|sdwan|...]
set interface {string}
end

```

config system fortiguard

Parameter	Description	Type	Size	Default
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of FortiGuard's Anycast network.		
	<i>disable</i>	Disable use of FortiGuard's Anycast network.		
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet
	Option	Description		
	<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.		
	<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.		
	<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.		
protocol	Protocol used to communicate with the FortiGuard servers.	option	-	https
	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).		

Parameter	Description	Type	Size	Default
port	Port used to communicate with the FortiGuard servers.	option	-	443
	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.		
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	-	enable
	Option	Description		
	enable	Enable automatic connection and login to FortiCloud.		
	disable	Disable automatic connection and login to FortiCloud.		
update-server-location	Signature update server location.	option	-	any
	Option	Description		
	usa	FGD servers in United States.		
	any	FGD servers in any location.		
sandbox-region	Cloud sandbox region.	string	Maximum length: 63	
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable
	Option	Description		
	enable	Enable Internet Service Database update.		
	disable	Disable Internet Service Database update.		
update-uwdb	Enable/disable allowlist update.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable allowlist update.		
	<i>disable</i>	Disable allowlist update.		
update-extdb	Enable/disable external resource update.	option	-	enable
	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
	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
	Option	Description		
	<i>enable</i>	Enable persistent connection to receive update notification from FortiGuard.		
	<i>disable</i>	Disable persistent connection to receive update notification from FortiGuard.		
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable
	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
	Option	Description		
	<i>enable</i>	Enable FortiGuard antispam request caching.		
	<i>disable</i>	Disable FortiGuard antispam request caching.		

Parameter	Description	Type	Size	Default						
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds . 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-mpercent	Maximum percent of FortiGate memory the antispam cache is allowed to use .	integer	Minimum value: 1 Maximum value: 15	2						
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 .	integer	Minimum value: 1 Maximum value: 30	7						
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable FortiGuard antivirus caching.</td></tr> <tr> <td><i>disable</i></td><td>Disable FortiGuard antivirus caching.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable FortiGuard antivirus caching.	<i>disable</i>	Disable FortiGuard antivirus caching.
Option	Description									
<i>enable</i>	Enable FortiGuard antivirus caching.									
<i>disable</i>	Disable FortiGuard antivirus caching.									
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries .	integer	Minimum value: 300 Maximum value: 86400	300						

Parameter	Description	Type	Size	Default						
outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use .	integer	Minimum value: 1 Maximum value: 15	2						
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 .	integer	Minimum value: 1 Maximum value: 30	7						
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.									
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable FortiGuard web filter caching.</td></tr> <tr> <td><i>disable</i></td><td>Disable FortiGuard web filter caching.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable FortiGuard web filter caching.	<i>disable</i>	Disable FortiGuard web filter caching.
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 .	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						

Parameter	Description	Type	Size	Default
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 .	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	-	

Option	Description	Type	Size	Default
<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	IP address of the proxy server.	ipv4-address	Not Specified	0.0.0.0
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	

Parameter	Description	Type	Size	Default
proxy-password	Proxy user password.	password	Not Specified	
videofilter-license	Interval of time between license checks for the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
videofilter-expiration	Expiration date of the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
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
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	

* This parameter may not exist in some models.

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>.	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			
enable	Allow the signatures specified by IDs to be triggered even if they are on hold.			
disable	Do not trigger the signatures that are on hold.			
<hr/>				

config system arp

IPv4 ARP table.

```
config system arp
  Description: IPv4 ARP table.
end
```

config system email-server

Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features.

```
config system email-server
  Description: Configure the email server used by the FortiGate various things. For example,
               for sending email messages to users to support user authentication features.
  set type {option}
  set reply-to {string}
  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|sdwan|...]
    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		
	custom	Use custom email server.		
reply-to	Reply-To email address.	string	Maximum length: 63	
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		
	enable	Enable authentication.		
	disable	Disable authentication.		
validate-server	Enable/disable validation of server certificate.	option	-	disable
	Option	Description		
	enable	Enable validation of server certificate.		
	disable	Disable validation of server certificate.		
username	SMTP server user name for authentication.	string	Maximum length: 63	
password	SMTP server user password for authentication.	password	Not Specified	
security	Connection security used by the email server.	option	-	none

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>starttls</i></td><td>STARTTLS.</td></tr> <tr> <td><i>smt�</i></td><td>SSL/TLS.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>starttls</i>	STARTTLS.	<i>smt�</i>	SSL/TLS.							
Option	Description															
<i>none</i>	None.															
<i>starttls</i>	STARTTLS.															
<i>smt�</i>	SSL/TLS.															
ssl-min Proto- version	Minimum supported protocol version for SSL/TLS connections .	option	-	default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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.			
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.															
interface- select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>auto</i></td> <td>Set outgoing interface automatically.</td> </tr> <tr> <td><i>sdwan</i></td> <td>Set outgoing interface by SD-WAN or policy routing rules.</td> </tr> <tr> <td><i>specify</i></td> <td>Set outgoing interface manually.</td> </tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

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 border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable alarm.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable alarm.</td> </tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable audible alarm.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable audible alarm.</td> </tr> </tbody> </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
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
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
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

Parameter	Description	Type	Size	Default
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
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 mac-address-table

Configure MAC address tables.

```
config system mac-address-table
  Description: Configure MAC address tables.
  edit <mac>
    set interface {string}
    set reply-substitute {mac-address}
  next
end
```

config system mac-address-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified	00:00:00:00:00:00

config system session-helper

Configure session helper.

```
config system session-helper
  Description: Configure session helper.
  edit <id>
    set name [ftp|tftp|...]
    set protocol {integer}
    set port {integer}
  next
end
```

config system session-helper

Parameter	Description	Type	Size	Default
name	Helper name.	option	-	
Option	Description			
<i>ftp</i>			FTP.	
<i>tftp</i>			TFTP.	
<i>ras</i>			RAS.	
<i>h323</i>			H323.	
<i>tns</i>			TNS.	
<i>mms</i>			MMS.	
<i>sip</i>			SIP.	
<i>pptp</i>			PPTP.	
<i>rtsp</i>			RTSP.	
<i>dns-udp</i>			DNS UDP.	
<i>dns-tcp</i>			DNS TCP.	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pmap</i>	PMAP.		
	<i>rsh</i>	RSH.		
	<i>dcerpc</i>	DCERPC.		
	<i>mgcp</i>	MGCP.		
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0

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
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 fips-cc

Configure FIPS-CC mode.

```

config system fips-cc
  Description: Configure FIPS-CC mode.
  set status [enable|disable]
  set entropy-token [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/fips-ciphers	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FIPS-CC mode.		
	<i>disable</i>	Disable FIPS-CC mode.		
entropy-token	Enable/disable/dynamic entropy token.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable entropy token to be present during boot process.		
	<i>disable</i>	Disable entropy token to be present during boot process.		
	<i>dynamic</i>	Dynamic detect entropy token to be present during boot process.		
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 tos-based-priority

Configure Type of Service (ToS) based priority table to set network traffic priorities.

```

config system tos-based-priority
  Description: Configure Type of Service (ToS) based priority table to set network traffic
  priorities.
  edit <id>
    set tos {integer}
    set priority [low|medium|...]

```

```
next  
end
```

config system tos-based-priority

Parameter	Description	Type	Size	Default
tos	Value of the ToS byte in the IP datagram header .	integer	Minimum value: 0 Maximum value: 15	0
priority	ToS based priority level to low, medium or high .	option	-	high
Option	Description			
<i>low</i>	Low priority.			
<i>medium</i>	Medium priority.			
<i>high</i>	High priority.			

config system dscp-based-priority

Configure DSCP based priority table.

```
config system dscp-based-priority
  Description: Configure DSCP based priority table.
  edit <id>
    set ds {integer}
    set priority [low|medium|...]
  next
end
```

config system dscp-based-priority

Parameter	Description	Type	Size	Default
ds	DSCP.	integer	Minimum value: 0 Maximum value: 63	0
priority	DSCP based priority level.	option	-	high
Option	Description			
<i>low</i>	Low priority.			
<i>medium</i>	Medium priority.			
<i>high</i>	High priority.			

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 respond.	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
Option		Description		
		<i>reinit</i> Reinitialize TTL.		
		<i>decrease</i> Decrease TTL.		
		<i>retain</i> Retain TTL.		
mode	SLA response mode.	option	-	none
Option		Description		
		<i>none</i> Disable probe.		
		<i>http-probe</i> HTTP probe.		
		<i>twamp</i> Two way active measurement protocol.		
security-mode	Twamp responder security mode.	option	-	none
Option		Description		
		<i>none</i> Unauthenticated mode.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<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 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 <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
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 <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
	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>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

Parameter	Description	Type	Size	Default
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 .	integer	Minimum value: 500 Maximum value: 3600000	500
probe-timeout	Time to wait before a probe packet is considered lost .	integer	Minimum value: 500 Maximum value: 5000	500
failtime	Number of retry attempts before the server is considered down	integer	Minimum value: 1 Maximum value: 3600	5
recoverytime	Number of successful responses received before server is considered recovered .	integer	Minimum value: 1 Maximum value: 3600	5
probe-count	Number of most recent probes that should be used to calculate latency and jitter .	integer	Minimum value: 5 Maximum value: 30	30
security-mode	Twamp controller security mode.	option	-	none

Parameter	Description	Type	Size	Default	
	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,	integer	Minimum value: 64 Maximum value: 1024	64	
ha-priority	HA election priority .	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	
	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	

Parameter	Description	Type	Size	Default
	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
dst	IP address of the server to be monitored.	string	Maximum length: 64	
protocol	Protocols used to monitor the server.	option	-	ping
	Option	Description		
	<i>ping</i>	PING link monitor.		
	<i>tcp-echo</i>	TCP echo link monitor.		
	<i>udp-echo</i>	UDP echo link monitor.		
	<i>http</i>	HTTP-GET link monitor.		
	<i>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

Parameter	Description	Type	Size	Default
weight	Weight of the monitor to this dst .	integer	Minimum value: 0 Maximum value: 255	0

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
Option		Description		
		enable Enable config.		
		disable Disable config.		
auto-install-image	Enable/disable auto install the image in USB disk.	option	-	disable
Option		Description		
		enable Enable config.		
		disable Disable config.		
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fgt_system.conf
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out

config system console

Configure console.

```
config system console
```

```

Description: Configure console.
set mode [batch|line]
set baudrate [9600|19200|...]
set output [standard|more]
set login [enable|disable]
set fortiexplorer [enable|disable]
end

```

config system console

Parameter	Description		Type	Size	Default												
mode	Console mode.		option	-	line												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>batch</i></td> <td>Batch mode.</td> </tr> <tr> <td><i>line</i></td> <td>Line mode.</td> </tr> </tbody> </table>		Option	Description	<i>batch</i>	Batch mode.	<i>line</i>	Line mode.									
Option	Description																
<i>batch</i>	Batch mode.																
<i>line</i>	Line mode.																
baudrate	Console baud rate.		option	-	9600												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>9600</td> <td>9600</td> </tr> <tr> <td>19200</td> <td>19200</td> </tr> <tr> <td>38400</td> <td>38400</td> </tr> <tr> <td>57600</td> <td>57600</td> </tr> <tr> <td>115200</td> <td>115200</td> </tr> </tbody> </table>		Option	Description	9600	9600	19200	19200	38400	38400	57600	57600	115200	115200			
Option	Description																
9600	9600																
19200	19200																
38400	38400																
57600	57600																
115200	115200																
output	Console output mode.		option	-	more												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>standard</i></td> <td>Standard output.</td> </tr> <tr> <td><i>more</i></td> <td>More page output.</td> </tr> </tbody> </table>		Option	Description	<i>standard</i>	Standard output.	<i>more</i>	More page output.									
Option	Description																
<i>standard</i>	Standard output.																
<i>more</i>	More page output.																
login	Enable/disable serial console and FortiExplorer.		option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Console login enable.</td> </tr> <tr> <td><i>disable</i></td> <td>Console login disable.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Console login enable.	<i>disable</i>	Console login disable.									
Option	Description																
<i>enable</i>	Console login enable.																
<i>disable</i>	Console login disable.																
fortiexplorer *	Enable/disable access for FortiExplorer.		option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable FortiExplorer access.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable FortiExplorer access.</td> </tr> </tbody> </table>		Option	Description	<i>enable</i>	Enable FortiExplorer access.	<i>disable</i>	Disable FortiExplorer access.									
Option	Description																
<i>enable</i>	Enable FortiExplorer access.																
<i>disable</i>	Disable FortiExplorer access.																

* This parameter may not exist in some models.

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 FortiGate to connect to any available third-party NTP server.
    edit <id>
      set server {string}
      set ntpv3 [enable|disable]
      set authentication [enable|disable]
      set key {password}
      set key-id {integer}
      set interface-select-method [auto|sdwan|...]
      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 FortiGate 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.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>custom</i>	Use any other available NTP server.			
syncinterval	NTP synchronization interval .	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 FortiGate NTP Server Mode. Your FortiGate becomes an NTP server for other devices on your network. The FortiGate relays NTP requests to its configured NTP server.	option	-	disable	
	Option	Description			
	<i>enable</i>	Enable FortiGate NTP Server Mode.			
	<i>disable</i>	Disable FortiGate NTP Server Mode.			
authentication	Enable/disable authentication.	option	-	disable	
	Option	Description			
	<i>enable</i>	Enable authentication.			
	<i>disable</i>	Disable authentication.			
key-type	Key type for authentication (MD5, SHA1).	option	-	MD5	
	Option	Description			
	<i>MD5</i>	Use MD5 to authenticate the message.			
	<i>SHA1</i>	Use SHA1 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>	FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services.	string	Maximum length: 79		

Parameter	Description	Type	Size	Default
Interface name.				

config ntpserver

Parameter	Description	Type	Size	Default								
server	IP address or hostname of the NTP Server.	string	Maximum length: 63									
ntp3v	Enable to use NTPv3 instead of NTPv4.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable NTPv3.</td></tr> <tr> <td><i>disable</i></td><td>Disable NTPv3 (use NTPv4).</td></tr> </tbody> </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 MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-	disable								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr> <tr> <td><i>disable</i></td><td>Disable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.	<i>disable</i>	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.		
Option	Description											
<i>enable</i>	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.											
<i>disable</i>	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.											
key	Key for MD5(NTPv3)/SHA1(NTPv4) authentication.	password	Not Specified									
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr> <tr> <td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr> <tr> <td><i>specify</i></td><td>Set outgoing interface manually.</td></tr> </tbody> </table>					Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

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 FortiGate system time by synchronizing with an PTP Server.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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							

Parameter	Description	Type	Size	Default
server-mode	Enable/disable FortiGate PTP server mode. Your FortiGate becomes an PTP server for other devices on your network.	option	-	disable
	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
server-interface-name	Interface name.	string	Maximum length: 15	
	Option	Description		
	<i>E2E</i>	End to end delay detection.		
	<i>P2P</i>	Peer to peer delay detection.		

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						
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiGate interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0						
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 FortiGate 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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>source</i></td><td>Source port match.</td></tr> <tr> <td><i>destination</i></td><td>Destination port match.</td></tr> </tbody> </table>				Option	Description	<i>source</i>	Source port match.	<i>destination</i>	Destination port match.
Option	Description									
<i>source</i>	Source port match.									
<i>destination</i>	Destination port match.									
server-type	Cache server type.	option	-	forward						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>forward</i></td><td>Forward server.</td></tr> <tr> <td><i>proxy</i></td><td>Proxy server.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable MD5 authentication.</td></tr> <tr> <td><i>disable</i></td><td>Disable MD5 authentication.</td></tr> </tbody> </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.									

Parameter	Description	Type	Size	Default										
password	Password for MD5 authentication.	password	Not Specified											
forward-method	Method used to forward traffic to the cache servers.	option	-	GRE										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>GRE</i></td><td>GRE encapsulation.</td></tr> <tr> <td><i>L2</i></td><td>L2 rewrite.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>auto</td></tr> <tr> <td><i>standard</i></td><td>Standard service.</td></tr> <tr> <td><i>dynamic</i></td><td>Dynamic service.</td></tr> </tbody> </table>	Option	Description	<i>auto</i>	auto	<i>standard</i>	Standard service.	<i>dynamic</i>	Dynamic service.					
Option	Description													
<i>auto</i>	auto													
<i>standard</i>	Standard service.													
<i>dynamic</i>	Dynamic service.													
primary-hash	Hash method.	option	-	dst-ip										
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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										

Parameter	Description	Type	Size	Default
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
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 FortiGate.	option	-	GRE
Option		Description		
		<i>GRE</i> GRE encapsulation.		
		<i>L2</i> L2 rewrite.		
		<i>any</i> GRE or L2.		
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 dns64

Configure DNS64.

```
config system dns64
```

```

Description: Configure DNS64.
set status [enable|disable]
set dns64-prefix {ipv6-prefix}
set always-synthesize-aaaa-record [enable|disable]
end

```

config system dns64

Parameter	Description	Type	Size	Default
status	Enable/disable DNS64 .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS64.		
	<i>disable</i>	Disable DNS64.		
dns64-prefix	DNS64 prefix must be ::/96 .	ipv6-prefix	Not Specified	64:ff9b::/96
always-synthesize-aaaa-record	Enable/disable AAAA record synthesis .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable AAAA record synthesis.		
	<i>disable</i>	Disable AAAA record synthesis.		

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
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable the RSSO RADIUS server for this VDOM.		
	<i>disable</i>	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 startup-error-log

Display startup config error on console.

```
config system startup-error-log
    Description: Display startup config error on console.
end
```

config system source-ip status

Show configured service source-IP.

```
config system source-ip status
    Description: Show configured service source-IP.
end
```

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 session-info list

List session.

```
config system session-info list
    Description: List session.
```

```
end
```

config system session-info expectation

List expectation session.

```
config system session-info expectation
    Description: List expectation session.
end
```

config system session-info full-stat

Fully stat session.

```
config system session-info full-stat
    Description: Fully stat session.
end
```

config system session-info statistics

Session statistics.

```
config system session-info statistics
    Description: Session statistics.
end
```

config system session-info ttl

TTL session.

```
config system session-info ttl
    Description: TTL session.
end
```

config system session-helper-info list

List session helper.

```
config system session-helper-info list
    Description: List session helper.
end
```

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 ftm-push

Configure FortiToken Mobile push services.

```
config system ftm-push
    Description: Configure FortiToken Mobile push services.
    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
server-port	Port to communicate with FortiToken Mobile push services server .	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_Factory **
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

Option	Description
enable	Enable FortiToken Mobile push services.
disable	Disable FortiToken Mobile push services.

** Values may differ between models.

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
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
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
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 fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
Description: Configure FortiSandbox.
```

```

set status [enable|disable]
set forticloud [enable|disable]
set server {string}
set source-ip {string}
set interface-select-method [auto|sdwan|...]
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
	Option	Description		
	<i>enable</i>	Enable FortiSandbox.		
	<i>disable</i>	Disable FortiSandbox.		
forticloud	Enable/disable FortiSandbox Cloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiSandbox Cloud.		
	<i>disable</i>	Disable FortiSandbox Cloud.		
server	Server address of the remote FortiSandbox.	string	Maximum length: 63	
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>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	
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	default

Parameter	Description	Type	Size	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.		
ssl-min Proto- version	Minimum supported protocol version for SSL/TLS connections .	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.		
email	Notifier email address.	string	Maximum length: 63	

config system fortiai

Configure FortiAI.

```
config system fortiai
  Description: Configure FortiAI.
  set status [disable|enable]
end
```

config system fortiai

Parameter	Description	Type	Size	Default
status	Enable/disable FortiAI.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable FortiAI.		
	<i>enable</i>	Enable FortiAI.		

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
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-	
Option	Description			
<i>log.fortianalyzer.setting</i>	<code>log.fortianalyzer.setting</code>			
<i>log.fortianalyzer.override-setting</i>	<code>log.fortianalyzer.override-setting</code>			
<i>log.fortianalyzer2.setting</i>	<code>log.fortianalyzer2.setting</code>			
<i>log.fortianalyzer2.override-setting</i>	<code>log.fortianalyzer2.override-setting</code>			
<i>log.fortianalyzer3.setting</i>	<code>log.fortianalyzer3.setting</code>			
<i>log.fortianalyzer3.override-setting</i>	<code>log.fortianalyzer3.override-setting</code>			
<i>log.fortianalyzer-cloud.setting</i>	<code>log.fortianalyzer-cloud.setting</code>			
<i>log.fortianalyzer-cloud.override-setting</i>	<code>log.fortianalyzer-cloud.override-setting</code>			
<i>log.syslogd.setting</i>	<code>log.syslogd.setting</code>			
<i>log.syslogd.override-setting</i>	<code>log.syslogd.override-setting</code>			
<i>log.syslogd2.setting</i>	<code>log.syslogd2.setting</code>			
<i>log.syslogd2.override-setting</i>	<code>log.syslogd2.override-setting</code>			
<i>log.syslogd3.setting</i>	<code>log.syslogd3.setting</code>			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>log.syslogd3.override-setting</i>	<i>log.syslogd3.override-setting</i>		
	<i>log.syslogd4.setting</i>	<i>log.syslogd4.setting</i>		
	<i>log.syslogd4.override-setting</i>	<i>log.syslogd4.override-setting</i>		
	<i>system.gre-tunnel</i>	<i>system.gre-tunnel</i>		
	<i>system.central-management</i>	<i>system.central-management</i>		
	<i>system.csf</i>	<i>system.csf</i>		
	<i>user.radius</i>	<i>user.radius</i>		
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-	all
	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 csf

Add this FortiGate to a Security Fabric or set up a new Security Fabric on this FortiGate.

```
config system csf
  Description: Add this FortiGate to a Security Fabric or set up a new Security Fabric on this
               FortiGate.
  set status [enable|disable]
  set upstream-ip {ipv4-address}
  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 downstream-accprofile {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]
    next
end
config fabric-connector
    Description: Fabric connector configuration.
    edit <serial>
        set accprofile {string}
        set configuration-write-access [enable|disable]
    next
end
config fabric-device
    Description: Fabric device configuration.
    edit <name>
        set device-ip {ipv4-address}
        set https-port {integer}
        set access-token {varlen_password}
    next
end
end

```

config system csf

Parameter	Description	Type	Size	Default
status	Enable/disable Security Fabric.	option	-	disable
	Option	Description		
	enable	Enable Security Fabric.		
	disable	Disable Security Fabric.		
upstream-ip	IP address of the FortiGate upstream from this FortiGate in the Security Fabric.	ipv4-address	Not Specified	0.0.0.0
upstream-port	The port number to use to communicate with the FortiGate upstream from this FortiGate in the Security Fabric .	integer	Minimum value: 1 Maximum value: 65535	8013
group-name	Security Fabric group name. All FortiGates in a Security Fabric must have the same group name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
group-password	Security Fabric group password. All FortiGates in a Security Fabric 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
	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
	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
	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
downstream-access	Enable/disable downstream device access to this device's configuration and data.	option	-	disable
	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.		
downstream-accprofile	Default access profile for requests from downstream devices.	string	Maximum length: 35	
configuration-sync	Configuration sync mode.	option	-	default

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Synchronize configuration for FortiAnalyzer, FortiSandbox, and Central Management to root node.		
	<i>local</i>	Do not synchronize configuration with root node.		
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default
	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
	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.		

config trusted-list

Parameter	Description	Type	Size	Default
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.		

Parameter	Description	Type	Size	Default
ha-members	HA members.	string	Maximum length: 19	
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable
	Option	Description		
	enable	Enable downstream authorization.		
	disable	Disable downstream authorization.		

config fabric-connector

Parameter	Description	Type	Size	Default
accprofile	Override access profile.	string	Maximum length: 35	
configuration-write-access	Enable/disable downstream device write access to configuration.	option	-	disable
	Option	Description		
	enable	Enable downstream device write access to configuration.		
	disable	Disable downstream device write access to configuration.		

config fabric-device

Parameter	Description	Type	Size	Default
device-ip	Device IP.	ipv4-address	Not Specified	0.0.0.0
https-port	HTTPS port for fabric device.	integer	Minimum value: 1 Maximum value: 65535	443
access-token	Device access token.	varlen_password	Not Specified	

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 license-type [forticare-support|fortiguard-webfilter|...]
set ioc-level [medium|high]
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}
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
description	Description.	var-string	Maximum length: 255	
trigger-type	Trigger type.	option	-	event-based
Option		Description		
		<i>event-based</i> Event based trigger. <i>scheduled</i> Scheduled trigger.		
event-type	Event type.	option	-	ioc
Option		Description		
		<i>ioc</i> Indicator of compromise detected. <i>event-log</i> Use log ID as trigger. <i>reboot</i> Device reboot.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>low-memory</i>	Conserve mode due to low memory.		
	<i>high-cpu</i>	High CPU usage.		
	<i>license-near-expiry</i>	License 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.		
license-type	License type.	option	-	forticare-support
	Option	Description		
	<i>forticare-support</i>	FortiCare support license.		
	<i>fortiguard-webfilter</i>	FortiGuard web filter license.		
	<i>fortiguard-antispam</i>	FortiGuard antispam license.		
	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.		
	<i>fortiguard-ips</i>	FortiGuard IPS license.		
	<i>fortiguard-management</i>	FortiGuard management service license.		
	<i>forticloud</i>	FortiCloud license.		
	<i>any</i>	Any license.		
ioc-level	IOC threat level.	option	-	high

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>medium</i>	IOC level medium and high.		
	<i>high</i>	IOC level high only.		
report-type	Security Rating report.	option	-	posture
	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 .	option	-	daily
	Option	Description		
	<i>hourly</i>	Run hourly.		
	<i>daily</i>	Run daily.		
	<i>weekly</i>	Run weekly.		
	<i>monthly</i>	Run monthly.		
trigger-weekday	Day of week for trigger.	option	-	
	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
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 .	integer	Minimum value: 0 Maximum value: 23	0
trigger-minute	Minute of the hour on which to trigger .	integer	Minimum value: 0 Maximum value: 59	0
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
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

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 tls-certificate {string}
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}
set headers <header1>, <header2>, ...
set verify-host-cert [enable|disable]
set script {var-string}
set accprofile {string}
set security-tag {string}
set sdn-connector <name1>, <name2>, ...
next
end

```

config system automation-action

Parameter	Description	Type	Size	Default
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 FortiOS dashboard alert.			
<i>disable-ssid</i>	Disable interface.			
<i>quarantine</i>	Quarantine host.			
<i>quarantine-forticlient</i>	Quarantine FortiClient by EMS.			
<i>quarantine-nsx</i>	Quarantine NSX instance.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
<code>tls-certificate</code>	Custom TLS certificate for API request.	string	Maximum length: 35	
<code>email-to <name></code>	Email addresses. Email address.	string	Maximum length: 255	
<code>email-from</code>	Email sender name.	var-string	Maximum length: 127	
<code>email-subject</code>	Email subject.	var-string	Maximum length: 511	
<code>minimum-interval</code>	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0
<code>aws-api-key</code>	AWS API Gateway API key.	password	Not Specified	
<code>azure-function-authorization</code>	Azure function authorization level.	option	-	anonymous

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>anonymous</i>	Anonymous authorization level (No authorization required).		
	<i>function</i>	Function authorization level (Function or Host Key required).		
	<i>admin</i>	Admin authorization level (Master Host Key required).		
azure-api-key	Azure function API key.	password	Not Specified	
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous
	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
	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
	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
	Option	Description		
	<i>http</i>	HTTP.		
	<i>https</i>	HTTPS.		
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-	post
	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
headers <header>	Request headers. Request header.	string	Maximum length: 255	
verify-host-cert	Enable/disable verification of the remote host certificate.	option	-	enable
	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	
accprofile	Access profile for CLI script action to access FortiGate features.	string	Maximum length: 35	
security-tag	NSX security tag.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79	

config system automation-destination

Automation destinations.

```
config system automation-destination
  Description: Automation destinations.
  edit <name>
    set type [fortigate|ha-cluster]
    set destination <name1>, <name2>, ...
    set ha-group-id {integer}
  next
end
```

config system automation-destination

Parameter	Description	Type	Size	Default
type	Destination type.	option	-	fortigate
Parameter	Description	Type	Size	Default
type	Destination type.	option	-	fortigate
destination <name>	Destinations. Destination.	string	Maximum length: 31	
ha-group-id	Cluster group ID set for this destination .	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}
    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
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	
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79	

config actions

Parameter	Description	Type	Size	Default
action	Action name.	string	Maximum length: 64	
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	0
required	Required in action chain.	option	-	disable
	Option	Description		
	<i>enable</i>	Required in action chain.		
	<i>disable</i>	Not required in action chain.		

config system nd-proxy

Configure IPv6 neighbor discovery proxy (RFC4389).

```

config system nd-proxy
  Description: Configure IPv6 neighbor discovery proxy (RFC4389).
  set status [enable|disable]
  set member <interface-name1>, <interface-name2>, ...
end

```

config system nd-proxy

Parameter	Description		Type	Size	Default
status	Enable/disable neighbor discovery proxy.		option	-	disable
	Option	Description			
	enable	Enable neighbor discovery proxy.			
	disable	Disable neighbor discovery proxy.			
member <interface- name>	Interfaces using the neighbor discovery proxy. Interface name.		string	Maximum length: 79	

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

```

config system saml

Parameter	Description	Type	Size	Default
status	Enable/disable SAML authentication .	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
prefix	Prefix.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
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
type	Type.	option	-	username
	Option	Description		
	<i>username</i>	User Name.		
	<i>email</i>	Email Address.		
	<i>profile-name</i>	Profile Name.		

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 upgrade-id {integer}
config node-list
    Description: Nodes which will be included in the upgrade.
    edit <serial>
        set timing [immediate|scheduled]
        set time {user}
        set setup-time {user}
        set upgrade-path {user}
        set device-type [fortigate|fortiswitch|...]
        set coordinating-fortigate {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>download-failed</i>	The image downloads failed. It will retry if possible.		
	<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>staging</i>	The upgrade is confirmed and images are being staged.		
	<i>final-check</i>	The upgrade is ready and final checks are in progress.		
	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.		
	<i>confirmed</i>	The upgrade was confirmed and reboots will begin soon.		
	<i>done</i>	The upgrade completed successfully.		
	<i>failed</i>	The upgrade failed due to a local issue.		
upgrade-id	Unique identifier for this upgrade.	integer	Minimum value: 0 Maximum value: 4294967295	0

config node-list

Parameter	Description	Type	Size	Default
timing	Whether the upgrade should be run immediately, or at a scheduled time.	option	-	immediate
	Option	Description		
	<i>immediate</i>	Begin the upgrade immediately.		
	<i>scheduled</i>	Begin the upgrade at a configured time.		
time	Scheduled time for the upgrade. Format hh:mm yyyy/mm/dd UTC.	user	Not Specified	
setup-time	When the upgrade was configured. Format hh:mm yyyy/mm/dd UTC.	user	Not Specified	
upgrade-path	Image IDs to upgrade through.	user	Not Specified	
device-type	What type of device this node represents.	option	-	fortigate
	Option	Description		
	<i>fortigate</i>	This device is a FortiGate.		
	<i>fortiswitch</i>	This device is a FortiSwitch.		
	<i>fortiap</i>	This device is a FortiAP.		
coordinating-fortigate	The serial of the FortiGate that controls this device	string	Maximum length: 79	

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 auto-asic-offload {enable|disable}
  set ipv4-address {ipv4-classnet-host}
  set br {ipv6-address}
  set update-url {string}
  set mode {map-e|fixed-ip}
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	
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
br	Border relay IPv6 address.	ipv6-address	Not Specified	::
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.		

* This parameter may not exist in some models.

config system ike

Configure IKE global attributes.

```
config system ike
  Description: Configure IKE global attributes.
```

```
set embryonic-limit {integer}
set dh-multiprocess [enable|disable]
set dh-worker-count {integer}
set dh-mode [software|hardware]
set dh-keypair-cache [enable|disable]
set dh-keypair-count {integer}
set dh-keypair-throttle [enable|disable]
config dh-group-1
    Description: Diffie-Hellman group 1 (MODP-768).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-2
    Description: Diffie-Hellman group 2 (MODP-1024).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-5
    Description: Diffie-Hellman group 5 (MODP-1536).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-14
    Description: Diffie-Hellman group 14 (MODP-2048).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-15
    Description: Diffie-Hellman group 15 (MODP-3072).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-16
    Description: Diffie-Hellman group 16 (MODP-4096).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-17
    Description: Diffie-Hellman group 17 (MODP-6144).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-18
    Description: Diffie-Hellman group 18 (MODP-8192).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
end
config dh-group-19
    Description: Diffie-Hellman group 19 (EC-P256).
```

```
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-20
Description: Diffie-Hellman group 20 (EC-P384).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-21
Description: Diffie-Hellman group 21 (EC-P521).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-27
Description: Diffie-Hellman group 27 (EC-P224BP).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-28
Description: Diffie-Hellman group 28 (EC-P256BP).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-29
Description: Diffie-Hellman group 29 (EC-P384BP).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-30
Description: Diffie-Hellman group 30 (EC-P512BP).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-31
Description: Diffie-Hellman group 31 (EC-X25519).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
config dh-group-32
Description: Diffie-Hellman group 32 (EC-X448).
set mode [software|hardware|...]
set keypair-cache [global|custom]
set keypair-count {integer}
end
end
```

config system ike

Parameter	Description	Type	Size	Default						
embryonic-limit	Maximum number of IPsec tunnels to negotiate simultaneously.	integer	Minimum value: 50 Maximum value: 20000	1000 **						
dh-multiprocess	Enable/disable multiprocess Diffie-Hellman daemon for IKE.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable multiprocess Diffie-Hellman for IKE.</td></tr> <tr> <td>disable</td><td>Disable multiprocess Diffie-Hellman for IKE.</td></tr> </tbody> </table>	Option	Description	enable	Enable multiprocess Diffie-Hellman for IKE.	disable	Disable multiprocess Diffie-Hellman for IKE.			
Option	Description									
enable	Enable multiprocess Diffie-Hellman for IKE.									
disable	Disable multiprocess Diffie-Hellman for IKE.									
dh-worker-count	Number of Diffie-Hellman workers to start.	integer	Minimum value: 1 Maximum value: 4 **	0						
dh-mode	Use software (CPU) or hardware (CPX) to perform Diffie-Hellman calculations.	option	-	hardware **						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>software</td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr> <tr> <td>hardware</td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr> </tbody> </table>	Option	Description	software	Prefer CPU to perform Diffie-Hellman calculations.	hardware	Prefer CPX to perform Diffie-Hellman calculations.			
Option	Description									
software	Prefer CPU to perform Diffie-Hellman calculations.									
hardware	Prefer CPX to perform Diffie-Hellman calculations.									
dh-keypair-cache	Enable/disable Diffie-Hellman key pair cache.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable Diffie-Hellman key pair cache.</td></tr> <tr> <td>disable</td><td>Disable Diffie-Hellman key pair cache.</td></tr> </tbody> </table>	Option	Description	enable	Enable Diffie-Hellman key pair cache.	disable	Disable Diffie-Hellman key pair cache.			
Option	Description									
enable	Enable Diffie-Hellman key pair cache.									
disable	Disable Diffie-Hellman key pair cache.									
dh-keypair-count	Number of key pairs to pre-generate for each Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	100 **						
dh-keypair-throttle	Enable/disable Diffie-Hellman key pair cache CPU throttling.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable Diffie-Hellman key pair cache CPU throttling.</td></tr> <tr> <td>disable</td><td>Disable Diffie-Hellman key pair cache CPU throttling.</td></tr> </tbody> </table>	Option	Description	enable	Enable Diffie-Hellman key pair cache CPU throttling.	disable	Disable Diffie-Hellman key pair cache CPU throttling.			
Option	Description									
enable	Enable Diffie-Hellman key pair cache CPU throttling.									
disable	Disable Diffie-Hellman key pair cache CPU throttling.									

** Values may differ between models.

config dh-group-1

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>software</i>		Prefer CPU to perform Diffie-Hellman calculations.		
<i>hardware</i>		Prefer CPX to perform Diffie-Hellman calculations.		
<i>global</i>		Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>global</i>		Use global Diffie-Hellman key pair cache setting.		
<i>custom</i>		Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-2

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>software</i>		Prefer CPU to perform Diffie-Hellman calculations.		
<i>hardware</i>		Prefer CPX to perform Diffie-Hellman calculations.		
<i>global</i>		Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>global</i>		Use global Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.			
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0	

config dh-group-5

Parameter	Description	Type	Size	Default	
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global	
	Option	Description			
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.			
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.			
	<i>global</i>	Use global dh-mode setting.			
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global	
	Option	Description			
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.			
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.			
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0	

config dh-group-14

Parameter	Description	Type	Size	Default	
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global	
	Option	Description			
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.			
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.			
	<i>global</i>	Use global dh-mode setting.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-15

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-16

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-17

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-18

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>software</i>		Prefer CPU to perform Diffie-Hellman calculations.		
<i>hardware</i>		Prefer CPX to perform Diffie-Hellman calculations.		
<i>global</i>		Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>global</i>		Use global Diffie-Hellman key pair cache setting.		
<i>custom</i>		Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-19

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>software</i>		Prefer CPU to perform Diffie-Hellman calculations.		
<i>hardware</i>		Prefer CPX to perform Diffie-Hellman calculations.		
<i>global</i>		Use global dh-mode setting.		

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-20

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-21

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-27

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default

Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-28

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>software</i>		Prefer CPU to perform Diffie-Hellman calculations.		
<i>hardware</i>		Prefer CPX to perform Diffie-Hellman calculations.		
<i>global</i>		Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>global</i>		Use global Diffie-Hellman key pair cache setting.		
<i>custom</i>		Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-29

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Option		Description		
<i>software</i>		Prefer CPU to perform Diffie-Hellman calculations.		
<i>hardware</i>		Prefer CPX to perform Diffie-Hellman calculations.		
<i>global</i>		Use global dh-mode setting.		

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-30

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-31

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config dh-group-32

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
Parameter	Description	Type	Size	Default

Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

config system acme

Configure ACME client.

```
config system acme
  Description: Configure ACME client.
  set interface <interface-name1>, <interface-name2>, ...
  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	

config accounts

Parameter	Description	Type	Size	Default
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	

test

This section includes syntax for the following commands:

- [config test wccpd on page 1244](#)
- [config test bfd on page 1254](#)
- [config test azd on page 1253](#)
- [config test sessionsync on page 1237](#)
- [config test dsd on page 1247](#)
- [config test smtp on page 1234](#)
- [config test forticron on page 1246](#)
- [config test sepm on page 1255](#)
- [config test csfd on page 1251](#)
- [config test syslogd on page 1238](#)
- [config test ocid on page 1253](#)
- [config test fds_notify on page 1257](#)
- [config test lnkmtd on page 1248](#)
- [config test pop3 on page 1235](#)
- [config test autod on page 1254](#)
- [config test ovrd on page 1239](#)
- [config test nntp on page 1236](#)
- [config test sflowd on page 1242](#)
- [config test openstackd on page 1255](#)
- [config test vned on page 1256](#)
- [config test pptpcd on page 1243](#)
- [config test sdhcd on page 1252](#)
- [config test imap on page 1235](#)
- [config test ipsmonitor on page 1240](#)
- [config test quarantined on page 1246](#)
- [config test ipsengine on page 1240](#)
- [config test uploadd on page 1246](#)
- [config test wiredapd on page 1251](#)
- [config test ipsufd on page 1245](#)
- [config test snmpd on page 1241](#)
- [config test kubed on page 1254](#)
- [config test lted on page 1245](#)
- [config test dhcprelay on page 1243](#)
- [config test forticld on page 1237](#)
- [config test fsvrd on page 1251](#)
- [config test l2tpcd on page 1243](#)
- [config test gcpd on page 1253](#)
- [config test radius-das on page 1250](#)
- [config test harelay on page 1236](#)

- [config test radiusd](#) on page 1244
- [config test acd](#) on page 1241
- [config test fas](#) on page 1255
- [config test updated](#) on page 1248
- [config test dnsproxy](#) on page 1242
- [config test iotd](#) on page 1239
- [config test init](#) on page 1242
- [config test wf_monitor](#) on page 1239
- [config test netxd](#) on page 1249
- [config test ipmc_sensord](#) on page 1247
- [config test awsd](#) on page 1249
- [config test wad](#) on page 1244
- [config test radvd](#) on page 1252
- [config test sfupgraded](#) on page 1257
- [config test mrd](#) on page 1250
- [config test sdnd](#) on page 1256
- [config test hasync](#) on page 1236
- [config test dhcp6r](#) on page 1248
- [config test fsd](#) on page 1245
- [config test fcnacd](#) on page 1252
- [config test fnbamd](#) on page 1249
- [config test ipamd](#) on page 1256
- [config test ipldbd](#) on page 1240
- [config test miglogd](#) on page 1238
- [config test ftpd](#) on page 1235
- [config test hatalk](#) on page 1237
- [config test zebos_launcher](#) on page 1250
- [config test urlfilter](#) on page 1238
- [config test dhcp6c](#) on page 1247
- [config test ddnscd](#) on page 1241

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: -1	

config test ftpd

FTP proxy.

```
config test ftpd
    Description: FTP proxy.
    set <Integer> {string}
end
```

config test ftpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

config test hatalk

HA talk daemon.

```
config test hatalk
    Description: HA talk daemon.
    set <Integer> {string}
end
```

config test hatalk

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

config test ovrd

Override daemon.

```
config test ovrd
    Description: Override daemon.
    set <Integer> {string}
end
```

config test ovrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

config test ipldbd

IP load balancing daemon.

```
config test ipldbd
    Description: IP load balancing daemon.
    set <Integer> {string}
end
```

config test ipldbd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test ddnscd

DDNS client daemon.

```
config test ddnscd
  Description: DDNS client daemon.
  set <Integer> {string}
end
```

config test ddnscd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

config test sflowd

sFlow daemon.

```
config test sflowd
    Description: sFlow daemon.
    set <Integer> {string}
end
```

config test sflowd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

config test lted



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61F. It is not available for FortiGate VM64.

USB LTE daemon.

```
config test lted
  Description: USB LTE daemon.
  set <Integer> {string}
end
```

config test lted

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

config test ipmc_sensord



This command is available for reference model(s) FortiGate 140E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61F. It is not available for FortiGate VM64.

Ipmc sensor daemon.

```
config test ipmc_sensord
    Description: Ipmc sensor daemon.
    set <Integer> {string}
end
```

config test ipmc_sensord

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

config test lnkmtd

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

config test zebos_launcher

ZEBOS Launcher daemon

```
config test zebos_launcher
    Description: ZEBOS Launcher daemon
    set <Integer> {string}
end
```

config test zebos_launcher

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

config test sdnacd

SDN Connector daemon.

```
config test sdnacd
    Description: SDN Connector daemon.
    set <Integer> {string}
end
```

config test sdnacd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

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: -1	

user

This section includes syntax for the following commands:

- [config user setting on page 1299](#)
- [config user exchange on page 1272](#)
- [config user saml on page 1285](#)
- [config user tacacs+ on page 1270](#)
- [config user group on page 1307](#)
- [config user quarantine on page 1305](#)
- [config user ldap on page 1274](#)
- [config user certificate on page 1258](#)
- [config user domain-controller on page 1281](#)
- [config user pop3 on page 1284](#)
- [config user password-policy on page 1295](#)
- [config user krb-keytab on page 1280](#)
- [config user security-exempt-list on page 1312](#)
- [config user peergrp on page 1305](#)
- [config user nac-policy on page 1312](#)
- [config user fss0 on page 1289](#)
- [config user fortitoken on page 1295](#)
- [config user fss0-polling on page 1293](#)
- [config user radius on page 1259](#)
- [config user peer on page 1303](#)
- [config user adgrp on page 1292](#)
- [config user local on page 1296](#)

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						
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable allowing the certificate user to authenticate with the FortiGate unit.	option	-	enable						
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable user.</td></tr> <tr> <td><i>disable</i></td><td>Disable user.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 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 all-usergroup [disable|enable]
    set use-management-vdom [enable|disable]
    set nas-ip {ipv4-address}
    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 password-encoding [auto|ISO-8859-1]
set acct-all-servers [enable|disable]
set switch-controller-acct-fast-framedip-detect {integer}
set interface-select-method [auto|sdwan|...]
set interface {string}
set switch-controller-service-type {option1}, {option2}, ...
set rsso [enable|disable]
set rsso-radius-server-port {integer}
set rsso-radius-response [enable|disable]
set rsso-validate-request-secret [enable|disable]
set rsso-secret {password}
set rsso-endpoint-attribute [User-Name|NAS-IP-Address|...]
set rsso-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 rsso-context-timeout {integer}
set rsso-log-period {integer}
set rsso-log-flags {option1}, {option2}, ...
set rsso-flush-ip-session [enable|disable]
set rsso-ep-one-ip-only [enable|disable]
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|sdwan|...]
        set interface {string}
    next
end
next
end

```

config user radius

Parameter	Description	Type	Size	Default
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	{<name_str ip_str>} secondary RADIUS CN domain name or IP.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
secondary-secret	Secret key to access the secondary server.	password	Not Specified							
tertiary-server	{<name_str ip_str>} tertiary RADIUS CN domain name or IP.	string	Maximum length: 63							
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified							
timeout	Time in seconds between re-sending authentication requests.	integer	Minimum value: 1 Maximum value: 300	5						
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>disable</td><td>Do not automatically include this server in a user group.</td></tr> <tr> <td>enable</td><td>Include this RADIUS server in every user group.</td></tr> </tbody> </table>					Option	Description	disable	Do not automatically include this server in a user group.	enable	Include this RADIUS server in every user group.
Option	Description									
disable	Do not automatically include this server in a user group.									
enable	Include this RADIUS server in every user group.									
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Send requests using the management VDOM.</td></tr> <tr> <td>disable</td><td>Send requests using the current VDOM.</td></tr> </tbody> </table>					Option	Description	enable	Send requests using the management VDOM.	disable	Send requests using the current VDOM.
Option	Description									
enable	Send requests using the management VDOM.									
disable	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						
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable RADIUS CoA.</td></tr> <tr> <td>disable</td><td>Disable RADIUS CoA.</td></tr> </tbody> </table>					Option	Description	enable	Enable RADIUS CoA.	disable	Disable RADIUS CoA.
Option	Description									
enable	Enable RADIUS CoA.									
disable	Disable RADIUS CoA.									

Parameter	Description	Type	Size	Default
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
Option		Description		
		<i>enable</i> Enable H3C compatibility.		
		<i>disable</i> Disable H3C compatibility.		
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto
Option		Description		
		<i>auto</i> Use PAP, MSCHAP_v2, and CHAP (in that order).		
		<i>ms_chap_v2</i> Microsoft Challenge Handshake Authentication Protocol version 2.		
		<i>ms_chap</i> Microsoft Challenge Handshake Authentication Protocol.		
		<i>chap</i> Challenge Handshake Authentication Protocol.		
		<i>pap</i> Password Authentication Protocol.		
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
Option		Description		
		<i>enable</i> Enable username case-sensitive.		
		<i>disable</i> Disable username case-sensitive.		
group-override-attr-type	RADIUS attribute type to override user group information.	option	-	
Option		Description		
		<i>filter-Id</i> Filter-Id		
		<i>class</i> Class		
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
password-renewal	Enable/disable password renewal.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable password renewal.		
	<i>disable</i>	Disable password renewal.		
password-encoding	Password encoding.	option	-	auto
	Option	Description		
	<i>auto</i>	Use original password encoding.		
	<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.		
acct-all-servers	Enable/disable sending of accounting messages to all configured servers .	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 .	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>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	
switch-controller-service-type	RADIUS service type.	option	-	

Parameter	Description	Type	Size	Default
	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.		
	<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.		
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable
	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
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

Parameter	Description	Type	Size	Default
	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 endpoint identifier from the RADIUS Start record.	option	-	Calling-Station-Id
	Option	Description		
	<i>User-Name</i>	Use this attribute.		
	<i>NAS-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Netmask</i>	Use this attribute.		
	<i>Filter-Id</i>	Use this attribute.		
	<i>Login-IP-Host</i>	Use this attribute.		
	<i>Reply-Message</i>	Use this attribute.		
	<i>Callback-Number</i>	Use this attribute.		
	<i>Callback-Id</i>	Use this attribute.		
	<i>Framed-Route</i>	Use this attribute.		
	<i>Framed-IPX-Network</i>	Use this attribute.		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-	
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		
	<i>Acct-Session-Id</i>	Use this attribute.		
	<i>Acct-Multi-Session-Id</i>	Use this attribute.		
sso-attribute-key	Key prefix for SSO group value in the SSO attribute.	string	Maximum length: 35	
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint.	option	-	enable
	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

Parameter	Description	Type	Size	Default
rsso-log-flags	Events to log.	option	-	protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other
Option				
<i>protocol-error</i>				
Enable this log type.				
<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
Option				
<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
Option				
<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.				

config accounting-server

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	{<name_str>ip_str} Server CN domain name or IP.	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
	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	

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 authen-type [mschap|chap|...]
set authorization [enable|disable]
set source-ip {string}
set interface-select-method [auto|sdwan|...]
set interface {string}
next
end

```

config user tacacs+

Parameter	Description	Type	Size	Default
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	
authen-type	Allowed authentication protocols/methods.	option	-	auto
Option	Description			
<i>mschap</i>	MSCHAP.			
<i>chap</i>	CHAP.			
<i>pap</i>	PAP.			
<i>ascii</i>	ASCII.			
<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).			
authorization	Enable/disable TACACS+ authorization.	option	-	disable
Option	Description			
<i>enable</i>	Enable TACACS+ authorization.			

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>disable</i>	Disable TACACS+ authorization.			
source-ip	source IP for communications 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>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		

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 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
server-name	MS Exchange server hostname.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
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.			
auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos
Option	Description			
<i>spnego</i>	Negotiate authentication.			
<i>ntlm</i>	NTLM authentication.			
<i>kerberos</i>	Kerberos authentication.			
auth-level	Authentication security level used for the RPC protocol layer.	option	-	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

Parameter	Description	Type	Size	Default
	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 .	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.		
auto- discover-kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable
	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 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 server-identity-check [enable|disable]
    set source-ip {ipv4-address}
    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 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-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-filter {string}
set search-type {option1}, {option2}, ...
set obtain-user-info [enable|disable]
set user-info-exchange-server {string}
set interface-select-method [auto|sdwan|...]
set interface {string}
set antiphish [enable|disable]
set password-attr {string}
next
end

```

config user ldap

Parameter	Description	Type	Size	Default
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	
server-identity-check	Enable/disable LDAP server identity check (verify server domain name/IP address against the server certificate).	option	-	enable
Option	Description			
enable	Enable server identity check.			

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>disable</i>	Disable server identity check.			
source-ip	FortiGate IP address to be used for communication with the LDAP server.	ipv4-address	Not Specified	0.0.0.0	
source-port	Source port to be used for communication with the LDAP server.	integer	Minimum value: 0 Maximum value: 65535	0	
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	
	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	
	Option	Description			
	<i>disable</i>	disable two-factor authentication.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.		
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	
	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.		
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-min Proto- version	Minimum supported protocol version for SSL/TLS connections .	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.		
ca-cert	CA certificate name.	string	Maximum length: 79	
port	Port to be used for communication with the LDAP server .	integer	Minimum value: 1 Maximum value: 65535	389
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable password expiry warnings.		
	<i>disable</i>	Disable password expiry warnings.		
password-renewal	Enable/disable online password renewal.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable online password renewal.		
	<i>disable</i>	Disable online password renewal.		
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-	same
	Option	Description		
	<i>same</i>	Same as UPN.		
	<i>strip</i>	Strip domain string from UPN.		
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	-	
	Option	Description		
	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.		
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<code>enable</code>	Enable obtaining of user information.		
	<code>disable</code>	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
	Option	Description		
	<code>auto</code>	Set outgoing interface automatically.		
	<code>sdwan</code>	Set outgoing interface by SD-WAN or policy routing rules.		
	<code>specify</code>	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		
	<code>enable</code>	Enable AntiPhishing credential backend.		
	<code>disable</code>	Disable AntiPhishing credential backend.		
password-attr	Name of attribute to get password hash.	string	Maximum length: 35	userPassword

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
pac-data	Enable/disable parsing PAC data in the ticket.		option	-	enable
	Option	Description			
	<i>enable</i>	Enable parsing PAC data in the ticket.			
	<i>disable</i>	Disable parsing PAC data in the ticket.			
principal	Kerberos service principal, e.g. HTTP/fgt.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 domain-controller

Configure domain controller entries.

```

config user domain-controller
    Description: Configure domain controller entries.
    edit <name>
        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|sdwan|...]
        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 replication-port {integer}
set ldap-server <name1>, <name2>, ...
set dns-srv-lookup [enable|disable]
set ad-mode [none|ds|...]
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
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	::
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535	445
source-ip-address	FortiGate IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-ip6	FortiGate IPv6 address to be used for communication with the domain controller.	ipv6-address	Not Specified	::
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
domain-name	Domain DNS name.	string	Maximum length: 255	
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	
dns-srv-lookup	Enable/disable DNS service lookup.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS service lookup.		
	<i>disable</i>	Disable DNS service lookup.		
ad-mode	Set Active Directory mode.	option	-	none
	Option	Description		
	<i>none</i>	The server is not configured as an Active Directory Domain Server (AD DS).		
	<i>ds</i>	The server is configured as an Active Directory Domain Server (AD DS).		
	<i>lds</i>	The server is an Active Directory Lightweight Domain Server (AD LDS).		
adlds-dn	AD LDS distinguished name.	string	Maximum length: 255	
adlds-ip-address	AD LDS IPv4 address.	ipv4-address	Not Specified	0.0.0.0
adlds-ip6	AD LDS IPv6 address.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
adlds-port	Port number of AD LDS service .	integer	Minimum value: 0 Maximum value: 65535	389

config extra-server

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 .	integer	Minimum value: 0 Maximum value: 65535	445
source-ip-address	FortiGate IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0

config user 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
server	{<name_str ip_str>} server domain name or IP.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535	0
secure	SSL connection.	option	-	starttls
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 .	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.		

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 adfs-claim [enable|disable]
    set user-claim-type [email|given-name|...]
    set group-claim-type [email|given-name|...]
  next
```

end

config user saml

Parameter	Description	Type	Size	Default
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	
digest-method	Digest Method Algorithm. .	option	-	sha1

Option	Description
<i>sha1</i>	Digest Method Algorithm is SHA1.
<i>sha256</i>	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
------------------	--	--------	---	---------

Option	Description
<i>enable</i>	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).
<i>disable</i>	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).

Parameter	Description	Type	Size	Default
adfs-claim	Enable/disable ADFS Claim for user/group attribute in assertion statement .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ADFS Claim for user/group attribute in assertion statement.		
	<i>disable</i>	Disable ADFS Claim for user/group attribute in assertion statement.		
user-claim-type	User name claim in assertion statement.	option	-	upn
	Option	Description		
	<i>email</i>	E-mail address of the user.		
	<i>given-name</i>	Given name of the user.		
	<i>name</i>	Unique name of the user.		
	<i>upn</i>	User principal name (UPN) of the user.		
	<i>common-name</i>	Common name of the user.		
	<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.		
	<i>group</i>	Group that the user is a member of.		
	<i>upn-adfs-1x</i>	User principal name (UPN) of the user.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	Option	Description		
	<i>email</i>	E-mail address of the user.		
	<i>given-name</i>	Given name of the user.		
	<i>name</i>	Unique name of the user.		
	<i>upn</i>	User principal name (UPN) of the user.		
	<i>common-name</i>	Common name of the user.		
	<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.		
	<i>group</i>	Group that the user is a member of.		
	<i>upn-adfs-1x</i>	User principal name (UPN) of the user.		
	<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.		

Parameter	Description	Type	Size	Default
Option	Description			
<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.			

config user fss0

Configure Fortinet Single Sign On (FSSO) agents.

```
config user fss0
  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 ssl-trusted-cert {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set interface-select-method [auto|sdwan|...]
    set interface {string}
  next
end
```

config user fss0

Parameter	Description	Type	Size	Default
type	Server type.	option	-	default

Parameter	Description	Type	Size	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. The collector agent can only accept passwords up to 15 characters in length.	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. The collector agent can only accept passwords up to 15 characters in length.	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. The collector agent can only accept passwords up to 15 characters in length.	password	Not Specified		
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63		

Parameter	Description	Type	Size	Default
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password4	Password of the fourth FSSO collector agent. The collector agent can only accept passwords up to 15 characters in length.	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. The collector agent can only accept passwords up to 15 characters in length.	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			
<i>enable</i>	Enable automatic fetching of groups from LDAP server.			
<i>disable</i>	Disable automatic fetching of groups from LDAP server.			
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180

Parameter	Description	Type	Size	Default	
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	
	Option	Description			
	enable	Enable use of SSL.			
	disable	Disable use of SSL.			
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	
	Option	Description			
	auto	Set outgoing interface automatically.			
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.			
	specify	Set outgoing interface manually.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15		

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
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 fss0-polling

Configure FSSO active directory servers for polling mode.

```
config user fss0-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
    set smbv1 [enable|disable]
    set smb-ntlmv1-auth [enable|disable]
  next
end
```

config user fss0-polling

Parameter	Description	Type	Size	Default
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 user fortitoken

Configure FortiToken.

```
config user fortitoken
    Description: Configure FortiToken.
    edit <serial-number>
        set status {active|lock}
        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
status	Status	option	-	active
Parameter	Description	Type	Size	Default
Parameter	Description	Type	Size	Default
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
reg-id	Device Reg ID.	string	Maximum length: 256	
os-ver	Device Mobile Version.	string	Maximum length: 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]
  next
end

```

config user password-policy

Parameter	Description	Type	Size	Default
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180
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
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-	disable
	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.		

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 username-sensitivity [disable|enable]
next
end

```

config user local

Parameter	Description	Type	Size	Default
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable allowing the local user to authenticate with the FortiGate unit.	option	-	enable
Option		Description		
		<i>enable</i>	Enable user.	
		<i>disable</i>	Disable user.	
type	Authentication method.	option	-	password
Option		Description		
		<i>password</i>	Password authentication.	
		<i>radius</i>	RADIUS server authentication.	
		<i>tacacs+</i>	TACACS+ server authentication.	
		<i>ldap</i>	LDAP server authentication.	
passwd	User's password.	password	Not Specified	
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35	
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	

Parameter	Description	Type	Size	Default												
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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													

Parameter	Description	Type	Size	Default
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
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	
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 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-timeout {integer}
set auth-timeout-type [idle-timeout|hard-timeout|...]
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|...]
end

```

config user setting

Parameter	Description	Type	Size	Default
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet
	Option	Description		
	<i>http</i>	Allow HTTP authentication.		
	<i>https</i>	Allow HTTPS authentication.		
	<i>ftp</i>	Allow FTP authentication.		
	<i>telnet</i>	Allow TELNET authentication.		
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35	
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

Parameter	Description	Type	Size	Default
	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
	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
	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
	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
	Option	Description		
	<i>always</i>	Always trigger firewall authentication on demand.		
	<i>implicitly</i>	Implicitly trigger firewall authentication on demand.		
auth-timeout	Time in minutes before the firewall user authentication timeout requires the user to re-authenticate.	integer	Minimum value: 1 Maximum value: 1440	5
auth-timeout-type	Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.	option	-	idle-timeout

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>idle-timeout</i>	Idle timeout.		
	<i>hard-timeout</i>	Hard timeout.		
	<i>new-session</i>	New session timeout.		
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate .	integer	Minimum value: 1 Maximum value: 30	3
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout
	Option	Description		
	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.		
	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.		
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
	Option	Description		
	<i>enable</i>	Enable per policy disclaimer.		
	<i>disable</i>	Disable per policy disclaimer.		

Parameter	Description	Type	Size	Default
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		

config auth-ports

Parameter	Description	Type	Size	Default
type	Service type.	option	-	http
	Option	Description		
	<i>http</i>	HTTP service.		
	<i>https</i>	HTTPS service.		
	<i>ftp</i>	FTP service.		
	<i>telnet</i>	TELNET service.		
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024

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 ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set ldap-mode [password|principal-name]
```

```

set ocsp-override-server {string}
set two-factor [enable|disable]
set passwd {password}
next
end

```

config user peer

Parameter	Description	Type	Size	Default
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
	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
	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.		
ldap-server	Name of an LDAP server defined under the user ldap command. Performs client access rights check.	string	Maximum length: 35	
ldap-username	Username for LDAP server bind.	string	Maximum length: 35	
ldap-password	Password for LDAP server bind.	password	Not Specified	
ldap-mode	Mode for LDAP peer authentication.	option	-	password

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>password</i>	Username/password.		
	<i>principal-name</i>	Principal name.		
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
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	

config user quarantine

Configure quarantine support.

```
config user quarantine
  Description: Configure quarantine support.
  set quarantine [enable|disable]
  set traffic-policy {string}
  set firewall-groups {string}
  config targets
```

```

Description: Quarantine entry to hold multiple MACs.
edit <entry>
    set description {string}
    config macs
        Description: Quarantine MACs.
        edit <mac>
            set description {string}
            set drop [disable|enable]
            set parent {string}
        next
    end
next
end
end

```

config user quarantine

Parameter	Description	Type	Size	Default
quarantine	Enable/disable quarantine.	option	-	enable
Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable quarantine.		
	<i>disable</i>	Disable quarantine.		
traffic-policy	Traffic policy for quarantined MACs.	string	Maximum length: 63	
firewall-groups	Firewall address group which includes all quarantine MAC address.	string	Maximum length: 79	

config targets

Parameter	Description	Type	Size	Default
description	Description for the quarantine entry.	string	Maximum length: 63	

config macs

Parameter	Description	Type	Size	Default
description	Description for the quarantine MAC.	string	Maximum length: 63	
drop	Enable/Disable dropping of quarantined device traffic	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Sends quarantined device traffic to FortiGate.		
	<i>enable</i>	Blocks quarantined device traffic to FortiGate.		
parent	Parent entry name.	string	Maximum length: 63	

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 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
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
Option		Description		
		<i>firewall</i> Firewall.		
		<i>fssso-service</i> Fortinet Single Sign-On Service.		
		<i>rsso</i> RADIUS based Single Sign-On Service.		
		<i>guest</i> 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
Option		Description		
		<i>enable</i> Enable auth-concurrent-override.		
		<i>disable</i> Disable auth-concurrent-override.		
auth-concurrent-value	Maximum number of concurrent authenticated connections per user .	integer	Minimum value: 0 Maximum value: 100	0
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default								
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511									
member <name>	Names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Group member name.	string	Maximum length: 511									
user-id	Guest user ID type.	option	-	email								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Enable setting.</td></tr> <tr> <td><i>enable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.					
Option	Description											
<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.											
sponsor	Set the action for the sponsor guest user field.	option	-	optional								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.											

Parameter	Description	Type	Size	Default						
email	Enable/disable the guest user email address field.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Enable setting.</td></tr> <tr> <td><i>enable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.			
Option	Description									
<i>disable</i>	Enable setting.									
<i>enable</i>	Disable setting.									
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Enable setting.</td></tr> <tr> <td><i>enable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.			
Option	Description									
<i>disable</i>	Enable setting.									
<i>enable</i>	Disable setting.									
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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							
expire-type	Determine when the expiration countdown begins.	option	-	immediately						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>immediately</i></td><td>Immediately.</td></tr> <tr> <td><i>first-successful-login</i></td><td>First successful login.</td></tr> </tbody> </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.	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: 500 **	0						
multiple-guest-add	Enable/disable addition of multiple guests.	option	-	disable						

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

** Values may differ between models.

config match

Parameter	Description	Type	Size	Default
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
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 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
description	Description.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
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 nac-policy

Configure NAC policy matching pattern to identify matching NAC devices.

```
config user nac-policy
    Description: Configure NAC policy matching pattern to identify matching NAC devices.
    edit <name>
        set description {string}
        set category [device|firewall-user|...]
        set status [enable|disable]
        set mac {string}
        set hw-vendor {string}
        set type {string}
```

```

set family {string}
set os {string}
set hw-version {string}
set sw-version {string}
set host {string}
set user {string}
set src {string}
set user-group {string}
set ems-tag {string}
set switch-fortilink {string}
set switch-scope <switch-id1>, <switch-id2>, ...
set switch-mac-policy {string}
set firewall-address {string}
set ssid-policy {string}
next
end

```

config user nac-policy

Parameter	Description	Type	Size	Default
description	Description for the NAC policy matching pattern.	string	Maximum length: 63	
category	Category of NAC policy.	option	-	device
Option		Description		
		<i>device</i> Device category.		
		<i>firewall-user</i> Firewall user category.		
		<i>ems-tag</i> EMS Tag category.		
status	Enable/disable NAC policy.	option	-	enable
Option		Description		
		<i>enable</i> Enable NAC policy.		
		<i>disable</i> Disable NAC policy.		
mac	NAC policy matching MAC address.	string	Maximum length: 17	
hw-vendor	NAC policy matching hardware vendor.	string	Maximum length: 15	
type	NAC policy matching type.	string	Maximum length: 15	
family	NAC policy matching family.	string	Maximum length: 31	

Parameter	Description	Type	Size	Default
os	NAC policy matching operating system.	string	Maximum length: 31	
hw-version	NAC policy matching hardware version.	string	Maximum length: 15	
sw-version	NAC policy matching software version.	string	Maximum length: 15	
host	NAC policy matching host.	string	Maximum length: 64	
user	NAC policy matching user.	string	Maximum length: 64	
src	NAC policy matching source.	string	Maximum length: 15	
user-group	NAC policy matching user group.	string	Maximum length: 35	
ems-tag	NAC policy matching EMS tag.	string	Maximum length: 79	
switch-fortilink	FortiLink interface for which this NAC policy belongs to.	string	Maximum length: 15	
switch-scope <switch-id>	List of managed FortiSwitches on which NAC policy can be applied. Managed FortiSwitch name from available options.	string	Maximum length: 79	
switch-mac-policy	switch-mac-policy action to be applied on the matched NAC policy.	string	Maximum length: 63	
firewall-address	Dynamic firewall address to associate MAC which match this policy.	string	Maximum length: 79	
ssid-policy	SSID policy to be applied on the matched NAC policy.	string	Maximum length: 35	

videofilter

This section includes syntax for the following commands:

- [config videofilter youtube-key on page 1315](#)
- [config videofilter youtube-channel-filter on page 1315](#)
- [config videofilter profile on page 1316](#)

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
key	Key.	string	Maximum length: 47	

config videofilter youtube-channel-filter

Configure YouTube channel filter.

```
config videofilter youtube-channel-filter
  Description: Configure YouTube channel filter.
  edit <id>
    set name {string}
    set comment {var-string}
    set default-action [allow|monitor|...]
    config entries
      Description: YouTube filter entries.
      edit <id>
        set comment {var-string}
        set action [allow|monitor|...]
        set channel-id {string}
      next
    end
    set log [enable|disable]
  next
end
```

config videofilter youtube-channel-filter

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
default-action	YouTube channel filter default action.	option	-	monitor
Option		Description		
		<i>allow</i> Allow videos to be accessed.		
		<i>monitor</i> Monitor videos.		
		<i>block</i> Block videos.		
log	Eanble/disable logging.	option	-	disable
Option		Description		
		<i>enable</i> Enable logging.		
		<i>disable</i> Disable logging.		

config entries

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
action	YouTube channel filter action.	option	-	monitor
Option		Description		
		<i>allow</i> Allow videos to be accessed.		
		<i>monitor</i> Monitor videos.		
		<i>block</i> Block videos.		
channel-id	Channel ID.	string	Maximum length: 255	

config videofilter profile

Configure VideoFilter profile.

```
config videofilter profile
  Description: Configure VideoFilter profile.
  edit <name>
```

```

set comment {var-string}
set youtube-channel-filter {integer}
config fortiguard-category
    Description: Configure FortiGuard categories.
    config filters
        Description: Configure VideoFilter FortiGuard category.
        edit <id>
            set action [allow|monitor|...]
            set category-id {integer}
            set log [enable|disable]
        next
    end
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						
comment	Comment.	var-string	Maximum length: 255							
youtube-channel-filter	Set YouTube channel filter.	integer	Minimum value: 0 Maximum value: 4294967295	0						
youtube	Enable/disable YouTube video source.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable YouTube source.</td></tr> <tr> <td><i>disable</i></td><td>Disable YouTube source.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable Vimeo source.</td></tr> <tr> <td><i>disable</i></td><td>Disable Vimeo source.</td></tr> </tbody> </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						

Parameter	Description	Type	Size	Default
	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
action	VideoFilter action.	option	-	monitor
	Option	Description		
	<i>allow</i>	Allow videos to be accessed.		
	<i>monitor</i>	Monitor videos.		
	<i>block</i>	Block videos.		
category-id	Category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		

voip

This section includes syntax for the following commands:

- [config voip profile on page 1319](#)

config voip profile

Configure VoIP profiles.

```
config voip profile
  Description: Configure VoIP profiles.
  edit <name>
    set feature-set [flow|proxy]
    set comment {var-string}
    config sip
      Description: SIP.
      set status [disable|enable]
      set rtp [disable|enable]
      set nat-port-range {user}
      set open-register-pinchole [disable|enable]
      set open-contact-pinchole [disable|enable]
      set strict-register [disable|enable]
      set register-rate {integer}
      set register-rate-track [none|src-ip|...]
      set invite-rate {integer}
      set invite-rate-track [none|src-ip|...]
      set max-dialogs {integer}
      set max-line-length {integer}
      set block-long-lines [disable|enable]
      set block-unknown [disable|enable]
      set call-keepalive {integer}
      set block-ack [disable|enable]
      set block-bye [disable|enable]
      set block-cancel [disable|enable]
      set block-info [disable|enable]
      set block-invite [disable|enable]
      set block-message [disable|enable]
      set block-notify [disable|enable]
      set block-options [disable|enable]
      set block-prack [disable|enable]
      set block-publish [disable|enable]
      set block-refer [disable|enable]
      set block-register [disable|enable]
      set block-subscribe [disable|enable]
      set block-update [disable|enable]
      set register-contact-trace [disable|enable]
      set open-via-pinchole [disable|enable]
      set open-record-route-pinchole [disable|enable]
      set rfc2543-branch [disable|enable]
      set log-violations [disable|enable]
      set log-call-summary [disable|enable]
```

```
set nat-trace [disable|enable]
set subscribe-rate {integer}
set subscribe-rate-track [none|src-ip|...]
set message-rate {integer}
set message-rate-track [none|src-ip|...]
set notify-rate {integer}
set notify-rate-track [none|src-ip|...]
set refer-rate {integer}
set refer-rate-track [none|src-ip|...]
set update-rate {integer}
set update-rate-track [none|src-ip|...]
set options-rate {integer}
set options-rate-track [none|src-ip|...]
set ack-rate {integer}
set ack-rate-track [none|src-ip|...]
set prack-rate {integer}
set prack-rate-track [none|src-ip|...]
set info-rate {integer}
set info-rate-track [none|src-ip|...]
set publish-rate {integer}
set publish-rate-track [none|src-ip|...]
set bye-rate {integer}
set bye-rate-track [none|src-ip|...]
set cancel-rate {integer}
set cancel-rate-track [none|src-ip|...]
set preserve-override [disable|enable]
set no-sdp-fixup [disable|enable]
set contact-fixup [disable|enable]
set max-idle-dialogs {integer}
set block-geo-red-options [disable|enable]
set hosted-nat-traversal [disable|enable]
set hnt-restrict-source-ip [disable|enable]
set max-body-length {integer}
set unknown-header [discard|pass|...]
set malformed-request-line [discard|pass|...]
set malformed-header-via [discard|pass|...]
set malformed-header-from [discard|pass|...]
set malformed-header-to [discard|pass|...]
set malformed-header-call-id [discard|pass|...]
set malformed-header-cseq [discard|pass|...]
set malformed-header-rack [discard|pass|...]
set malformed-header-rseq [discard|pass|...]
set malformed-header-contact [discard|pass|...]
set malformed-header-record-route [discard|pass|...]
set malformed-header-route [discard|pass|...]
set malformed-header-expires [discard|pass|...]
set malformed-header-content-type [discard|pass|...]
set malformed-header-content-length [discard|pass|...]
set malformed-header-max-forwards [discard|pass|...]
set malformed-header-allow [discard|pass|...]
set malformed-header-p-asserted-identity [discard|pass|...]
set malformed-header-no-require [discard|pass|...]
set malformed-header-no-proxy-require [discard|pass|...]
set malformed-header-sdp-v [discard|pass|...]
set malformed-header-sdp-o [discard|pass|...]
set malformed-header-sdp-s [discard|pass|...]
set malformed-header-sdp-i [discard|pass|...]
```

```

set malformed-header-sdp-c [discard|pass|...]
set malformed-header-sdp-b [discard|pass|...]
set malformed-header-sdp-z [discard|pass|...]
set malformed-header-sdp-k [discard|pass|...]
set malformed-header-sdp-a [discard|pass|...]
set malformed-header-sdp-t [discard|pass|...]
set malformed-header-sdp-r [discard|pass|...]
set malformed-header-sdp-m [discard|pass|...]
set provisional-invite-expiry-time {integer}
set ips-rtp [disable|enable]
set ssl-mode [off|full]
set ssl-send-empty-frags [enable|disable]
set ssl-client-renegotiation [allow|deny|...]
set ssl-algorithm [high|medium|...]
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-client-certificate {string}
set ssl-server-certificate {string}
set ssl-auth-client {string}
set ssl-auth-server {string}
end
config sccp
    Description: SCCP.
    set status [disable|enable]
    set block-mcast [disable|enable]
    set verify-header [disable|enable]
    set log-call-summary [disable|enable]
    set log-violations [disable|enable]
    set max-calls {integer}
end
next
end

```

config voip profile

Parameter	Description	Type	Size	Default
feature-set	Flow or proxy inspection feature set.	option	-	proxy
	Option	Description		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
comment	Comment.	var-string	Maximum length: 255	

config sip

Parameter	Description	Type	Size	Default
status	Enable/disable SIP.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
rtp	Enable/disable create pinholes for RTP traffic to traverse firewall.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
nat-port-range	RTP NAT port range.	user	Not Specified	5117-65533
open-register-pinhole	Enable/disable open pinhole for REGISTER Contact port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-contact-pinhole	Enable/disable open pinhole for non-REGISTER Contact port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
strict-register	Enable/disable only allow the registrar to connect.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
register-rate	REGISTER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default								
register-rate-track	Track the packet protocol field.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>src-ip</i></td><td>Source IP.</td></tr> <tr> <td><i>dest-ip</i></td><td>Destination IP.</td></tr> </tbody> </table>				Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
invite-rate	INVITE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
invite-rate-track	Track the packet protocol field.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>src-ip</i></td><td>Source IP.</td></tr> <tr> <td><i>dest-ip</i></td><td>Destination IP.</td></tr> </tbody> </table>				Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
max-dialogs	Maximum number of concurrent calls/dialogs (per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-line-length	Maximum SIP header line length .	integer	Minimum value: 78 Maximum value: 4096	998								
block-long-lines	Enable/disable block requests with headers exceeding max-line-length.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable status.</td></tr> <tr> <td><i>enable</i></td><td>Enable status.</td></tr> </tbody> </table>				Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
block-unknown	Block unrecognized SIP requests .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable status.</td></tr> </tbody> </table>				Option	Description	<i>disable</i>	Disable status.				
Option	Description											
<i>disable</i>	Disable status.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status.		
call-keepalive	Continue tracking calls with no RTP for this many minutes.	integer	Minimum value: 0 Maximum value: 10080	0
block-ack	Enable/disable block ACK requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-bye	Enable/disable block BYE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-cancel	Enable/disable block CANCEL requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-info	Enable/disable block INFO requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-invite	Enable/disable block INVITE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-message	Enable/disable block MESSAGE requests.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-notify	Enable/disable block NOTIFY requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-options	Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-prack	Enable/disable block prack requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-publish	Enable/disable block PUBLISH requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-refer	Enable/disable block REFER requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-register	Enable/disable block REGISTER requests.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-subscribe	Enable/disable block SUBSCRIBE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-update	Enable/disable block UPDATE requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
register-contact-trace	Enable/disable trace original IP/port within the contact header of REGISTER requests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-via-pinhole	Enable/disable open pinhole for Via port.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-record-route-pinhole	Enable/disable open pinhole for Record-Route port.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
rfc2543-branch	Enable/disable support via branch compliant with RFC 2543.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of SIP violations.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-call-summary	Enable/disable logging of SIP call summary.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
nat-trace	Enable/disable preservation of original IP in SDP i line.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
subscribe-rate	SUBSCRIBE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
subscribe-rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		

Parameter	Description	Type	Size	Default
message-rate	MESSAGE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
message-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.		
notify-rate	NOTIFY request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
notify-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		
refer-rate	REFER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
refer-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		

Parameter	Description	Type	Size	Default
update-rate	UPDATE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
update-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		
options-rate	OPTIONS request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
options-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		
ack-rate	ACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
ack-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		

Parameter	Description	Type	Size	Default
prack-rate	PRACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
prack-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		
info-rate	INFO request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
info-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		
publish-rate	PUBLISH request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
publish-rate-track	Track the packet protocol field.	option	-	none
Option		Description		
<i>none</i>		None.		
<i>src-ip</i>		Source IP.		
<i>dest-ip</i>		Destination IP.		

Parameter	Description	Type	Size	Default								
bye-rate	BYE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
bye-rate-track	Track the packet protocol field.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>src-ip</i></td><td>Source IP.</td></tr> <tr> <td><i>dest-ip</i></td><td>Destination IP.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
cancel-rate	CANCEL request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
cancel-rate-track	Track the packet protocol field.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>none</i></td><td>None.</td></tr> <tr> <td><i>src-ip</i></td><td>Source IP.</td></tr> <tr> <td><i>dest-ip</i></td><td>Destination IP.</td></tr> </tbody> </table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
preserve-override	Override i line to preserve original IPS .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable status.</td></tr> <tr> <td><i>enable</i></td><td>Enable status.</td></tr> </tbody> </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.											
no-sdp-fixup	Enable/disable no SDP fix-up.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable status.</td></tr> <tr> <td><i>enable</i></td><td>Enable status.</td></tr> </tbody> </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.											
contact-fixup	Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-idle-dialogs	Maximum number established but idle dialogs to retain (per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
block-geo-red-options	Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
hosted-nat-traversal	Hosted NAT Traversal (HNT).	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
hnt-restrict-source-ip	Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-body-length	Maximum SIP message body length (0 meaning no limit).	integer	Minimum value: 0 Maximum value: 4294967295	0
unknown-header	Action for unknown SIP header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-request-line	Action for malformed request line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-via	Action for malformed VIA header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-from	Action for malformed From header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-to	Action for malformed To header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-call-id	Action for malformed Call-ID header.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-cseq	Action for malformed CSeq header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-rack	Action for malformed RAck header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-rseq	Action for malformed RSeq header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-contact	Action for malformed Contact header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-record-route	Action for malformed Record-Route header.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-route	Action for malformed Route header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-expires	Action for malformed Expires header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-content-type	Action for malformed Content-Type header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-content-length	Action for malformed Content-Length header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		

Parameter	Description	Type	Size	Default
malformed-header-max-forwards	Action for malformed Max-Forwards header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-allow	Action for malformed Allow header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-p asserted-identity	Action for malformed P-Asserted-Identity header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-no-require	Action for malformed SIP messages without Require header.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-no-proxy-require	Action for malformed SIP messages without Proxy-Require header.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-v	Action for malformed SDP v line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-o	Action for malformed SDP o line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-s	Action for malformed SDP s line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-i	Action for malformed SDP i line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-c	Action for malformed SDP c line.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-b	Action for malformed SDP b line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-z	Action for malformed SDP z line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-k	Action for malformed SDP k line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-a	Action for malformed SDP a line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-t	Action for malformed SDP t line.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-r	Action for malformed SDP r line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-m	Action for malformed SDP m line.	option	-	pass
	Option	Description		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
provisional-invite-expiry-time	Expiry time for provisional INVITE.	integer	Minimum value: 10 Maximum value: 3600	210
ips-rtp	Enable/disable allow IPS on RTP.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
ssl-mode	SSL/TLS mode for encryption & decryption of traffic.	option	-	off
	Option	Description		
	<i>off</i>	No SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		
ssl-send-empty-frags	Send empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Send empty fragments.		
	<i>disable</i>	Do not send empty fragments.		
ssl-client-renegotiation	Allow/block client renegotiation by server.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow a SSL client to renegotiate.		
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.		
	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.		
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option	Description		
	<i>high</i>	High encryption. Allow only AES and ChaCha.		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-pfs	SSL Perfect Forward Secrecy.	option	-	allow
	Option	Description		
	<i>require</i>	PFS mandatory.		
	<i>deny</i>	PFS rejected.		
	<i>allow</i>	PFS allowed.		
ssl-min-version	Lowest SSL/TLS version to negotiate.	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 to negotiate.	option	-	tls-1.3

Parameter	Description		Type	Size	Default
	Option	Description			
	<i>ssl-3.0</i>	SSL 3.0.			
	<i>tls-1.0</i>	TLS 1.0.			
	<i>tls-1.1</i>	TLS 1.1.			
	<i>tls-1.2</i>	TLS 1.2.			
	<i>tls-1.3</i>	TLS 1.3.			
ssl-client-certificate	Name of Certificate to offer to server if requested.	string		Maximum length: 35	
ssl-server-certificate	Name of Certificate return to the client in every SSL connection.	string		Maximum length: 35	
ssl-auth-client	Require a client certificate and authenticate it with the peer/peergrp.	string		Maximum length: 35	
ssl-auth-server	Authenticate the server's certificate with the peer/peergrp.	string		Maximum length: 35	

config sccp

Parameter	Description		Type	Size	Default
	Option	Description			
status	Enable/disable SCCP.	option	-		enable
	<i>disable</i>	Disable status.			
	<i>enable</i>	Enable status.			
block-mcast	Enable/disable block multicast RTP connections.	option	-		disable
	<i>disable</i>	Disable status.			
	<i>enable</i>	Enable status.			
verify-header	Enable/disable verify SCCP header content.	option	-		disable
	<i>disable</i>	Disable status.			
	<i>enable</i>	Enable status.			
log-call-summary	Enable/disable log summary of SCCP calls.	option	-		disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of SCCP violations.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-calls	Maximum calls per minute per SCCP client (max 65535).	integer	Minimum value: 0 Maximum value: 65535	0

vpn

This section includes syntax for the following commands:

- [config vpn ssl web host-check-software](#) on page 1357
- [config vpn ipsec manualkey-interface](#) on page 1465
- [config vpn ssl web realm](#) on page 1356
- [config vpn ipsec phase2](#) on page 1421
- [config vpn ipsec concentrator](#) on page 1432
- [config vpn ipsec stats tunnel](#) on page 1468
- [config vpn ipsec phase2-interface](#) on page 1456
- [config vpn certificate local](#) on page 1346
- [config vpn ipsec manualkey](#) on page 1430
- [config vpn ssl web portal](#) on page 1359
- [config vpn ssl client](#) on page 1401
- [config vpn certificate ca](#) on page 1344
- [config vpn status ssl hw-acceleration-status](#) on page 1476
- [config vpn certificate crl](#) on page 1349
- [config vpn certificate setting](#) on page 1351
- [config vpn l2tp](#) on page 1470
- [config vpn ssl web user-group-bookmark](#) on page 1376
- [config vpn ipsec forticlient](#) on page 1467
- [config vpn certificate ocsp-server](#) on page 1351
- [config vpn ssl settings](#) on page 1388
- [config vpn ipsec tunnel name](#) on page 1469
- [config vpn certificate remote](#) on page 1345
- [config vpn ipsec phase1-interface](#) on page 1432
- [config vpn ike gateway](#) on page 1475
- [config vpn status l2tp](#) on page 1475
- [config vpn ipsec tunnel details](#) on page 1468
- [config vpn ipsec stats crypto](#) on page 1468
- [config vpn pptp](#) on page 1469
- [config vpn ssl web user-bookmark](#) on page 1382
- [config vpn ipsec tunnel summary](#) on page 1468
- [config vpn status ssl list](#) on page 1476
- [config vpn status pptp](#) on page 1475
- [config vpn ovpn](#) on page 1471
- [config vpn ipsec phase1](#) on page 1402
- [config vpn ssl monitor](#) on page 1402

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 auto-update-days {integer}
        set auto-update-days-warning {integer}
        set source-ip {ipv4-address}
    next
end
```

config vpn certificate ca

Parameter	Description	Type	Size	Default
ca	CA certificate as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the CA certificate.	option	-	vdom
Option		Description		
		<i>global</i>	Global range.	
		<i>vdom</i>	VDOM IP address range.	
source	CA certificate source type.	option	-	user
Option		Description		
		<i>factory</i>	Factory installed certificate.	
		<i>user</i>	User generated certificate.	
		<i>bundle</i>	Bundle file certificate.	
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
Option		Description		
		<i>enable</i>	Trusted CA for SSL inspection.	
		<i>disable</i>	Untrusted CA for SSL inspection.	

Parameter	Description	Type	Size	Default
scep-url	URL of the SCEP server.	string	Maximum length: 255	
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated .	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

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
remote	Remote certificate.	user	Not Specified	
range	Either the global or VDOM IP address range for the remote certificate.	option	-	vdom
Option		Description		
		<i>global</i> Global range.		
		<i>vdom</i> VDOM IP address range.		
source	Remote certificate source type.	option	-	user

Parameter	Description	Type	Size	Default
Option	Description			
<i>factory</i>	Factory installed certificate.			
<i>user</i>	User generated certificate.			
<i>bundle</i>	Bundle file certificate.			

config vpn certificate local

Local keys and certificates.

```
config vpn certificate local
  Description: Local keys and certificates.
  edit <name>
    set password {password}
    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 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}
  next
end
```

config vpn certificate local

Parameter	Description	Type	Size	Default
password	Password as a PEM file.	password		Not Specified

Parameter	Description	Type	Size	Default								
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									
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>global</i></td><td>Global range.</td></tr> <tr> <td><i>vdom</i></td><td>VDOM IP address range.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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									

Parameter	Description	Type	Size	Default
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
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 FortiGate uses for authentication as a VPN client.	string	Maximum length: 63	
ike-localid-type	IKE local ID type.	option	-	asn1dn
Option		Description		
		<i>asn1dn</i> ASN.1 distinguished name.		
		<i>fqdn</i> Fully qualified domain name.		
enroll-protocol	Certificate enrollment protocol.	option	-	none
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.		
cmp-server	'ADDRESS:PORT' for CMP server.	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>keyupdate</i>	Key Update.		
	<i>renewal</i>	Renewal.		
acme-ca-url	The URL for the ACME CA server .	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this Fortigate.	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 .	integer	Minimum value: 1 Maximum value: 60	30

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
crl	Certificate Revocation List as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the certificate.	option	-	vdom
Option		Description		
		<i>global</i>	Global range.	
		<i>vdom</i>	VDOM IP address range.	
source	Certificate source type.	option	-	user
Option		Description		
		<i>factory</i>	Factory installed certificate.	
		<i>user</i>	User generated certificate.	
		<i>bundle</i>	Bundle file certificate.	
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 FortiGate 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 ocsp-server

OCSP server configuration.

```
config vpn certificate ocsp-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 {ipv4-address}
    next
end
```

config vpn certificate ocsp-server

Parameter	Description	Type	Size	Default
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
	Option	Description		
	revoke	Revoke certificate if server is unavailable.		
	ignore	Ignore OCSP check if server is unavailable.		
source-ip	Source IP address for communications to the OCSP server.	ipv4-address	Not Specified	0.0.0.0

config vpn certificate setting

VPN certificate setting.

```
config vpn certificate setting
    Description: VPN certificate setting.
    set ocsp-status [enable|disable]
    set ocsp-option [certificate|server]
    set ssl-ocsp-source-ip {ipv4-address}
    set ocsp-default-server {string}
```

```

set interface-select-method [auto|sdwan|...]
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 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
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-	server
	Option	Description		
	<i>certificate</i>	Use URL from certificate.		
	<i>server</i>	Use URL from configured OCSP server.		
ssl-ocsp-source-ip	Source IP address to use to communicate with the OCSP server.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default								
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr> <tr> <td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr> <tr> <td><i>specify</i></td><td>Set outgoing interface manually.</td></tr> </tbody> </table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
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 .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	substring								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 .	option	-	subset								

Parameter	Description	Type	Size	Default
	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	option	-	substring
	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 mutliple CN fields in certificate subject name .	option	-	enable
	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-proto-version	Minimum supported protocol version for SSL/TLS connections .	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.		

Parameter	Description	Type	Size	Default
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode .	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 .	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.		
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

Parameter	Description	Type	Size	Default
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 .	option	-	ignore
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 .	option	-	ignore
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 .	option	-	ignore
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 ssl web realm

Realm.

```
config vpn ssl web realm
  Description: Realm.
  edit <url-path>
    set max-concurrent-user {integer}
    set login-page {var-string}
    set virtual-host {var-string}
    set virtual-host-only [enable|disable]
    set radius-server {string}
    set nas-ip {ipv4-address}
    set radius-port {integer}
  next
```

end

config vpn ssl web realm

Parameter	Description	Type	Size	Default
max-concurrent-user	Maximum concurrent users .	integer	Minimum value: 0 Maximum value: 65535	0
login-page	Replacement HTML for SSL-VPN login page.	var-string	Maximum length: 32768	
virtual-host	Virtual host name for realm.	var-string	Maximum length: 255	
virtual-host-only	Enable/disable enforcement of virtual host method for SSL-VPN client access.	option	-	disable
Option	Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
radius-server	RADIUS server associated with realm.	string	Maximum length: 35	
nas-ip	IP address used as a NAS-IP to communicate with the RADIUS server.	ipv4-address	Not Specified	0.0.0.0
radius-port	RADIUS service port number .	integer	Minimum value: 0 Maximum value: 65535	0

config vpn ssl web host-check-software

SSL-VPN host check software.

```
config vpn ssl web host-check-software
  Description: SSL-VPN host check software.
  edit <name>
    set os-type [windows|macos]
    set type [av|fw]
    set version {string}
    set guid {user}
    config check-item-list
      Description: Check item list.
      edit <id>
```

```

        set action [require|deny]
        set type [file|registry|...]
        set target {string}
        set version {string}
        set md5s <id1>, <id2>, ...
    next
end
next
end

```

config vpn ssl web host-check-software

Parameter	Description		Type	Size	Default
os-type	OS type.		option	-	windows
	Option	Description			
	windows	Microsoft Windows operating system.			
	macos	Apple MacOS operating system.			
type	Type.		option	-	av
	Option	Description			
	av	AntiVirus.			
	fw	Firewall.			
version	Version.		string	Maximum length: 35	
guid	Globally unique ID.		user	Not Specified	

config check-item-list

Parameter	Description		Type	Size	Default
action	Action.		option	-	require
	Option	Description			
	require	Require.			
	deny	Deny.			
type	Type.		option	-	file
	Option	Description			
	file	File.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>registry</i>	Registry.		
	<i>process</i>	Process.		
target	Target.	string	Maximum length: 255	
version	Version.	string	Maximum length: 35	
md5s <id>	MD5 checksum. Hex string of MD5 checksum.	string	Maximum length: 32	

config vpn ssl web portal

Portal.

```
config vpn ssl web portal
  Description: Portal.
  edit <name>
    set tunnel-mode [enable|disable]
    set ip-mode [range|user-group]
    set auto-connect [enable|disable]
    set keep-alive [enable|disable]
    set save-password [enable|disable]
    set ip-pools <name1>, <name2>, ...
    set exclusive-routing [enable|disable]
    set service-restriction [enable|disable]
    set split-tunneling [enable|disable]
    set split-tunneling-routing-negate [enable|disable]
    set split-tunneling-routing-address <name1>, <name2>, ...
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-suffix {var-string}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
    set ipv6-tunnel-mode [enable|disable]
    set ipv6-pools <name1>, <name2>, ...
    set ipv6-exclusive-routing [enable|disable]
    set ipv6-service-restriction [enable|disable]
    set ipv6-split-tunneling [enable|disable]
    set ipv6-split-tunneling-routing-negate [enable|disable]
    set ipv6-split-tunneling-routing-address <name1>, <name2>, ...
    set ipv6-dns-server1 {ipv6-address}
    set ipv6-dns-server2 {ipv6-address}
    set ipv6-wins-server1 {ipv6-address}
    set ipv6-wins-server2 {ipv6-address}
    set web-mode [enable|disable]
    set display-bookmark [enable|disable]
    set user-bookmark [enable|disable]
    set allow-user-access {option1}, {option2}, ...
```

```
set user-group-bookmark [enable|disable]
config bookmark-group
    Description: Portal bookmark group.
    edit <name>
        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 additional-params {var-string}
                set description {var-string}
                set keyboard-layout [ar-101|ar-102|...]
                set security [rdp|nla|...]
                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|static|...]
            config form-data
                Description: Form data.
                edit <name>
                    set value {var-string}
                    next
                end
            end
            set sso-credential [sslvpn-login|alternative]
            set sso-username {var-string}
            set sso-password {password}
            set sso-credential-sent-once [enable|disable]
        next
    end
next
end
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set rewrite-ip-uri-ui [enable|disable]
set heading {string}
set redir-url {var-string}
set theme [jade|neutrino|...]
set custom-lang {string}
set smb-ntlmv1-auth [enable|disable]
set smbv1 [enable|disable]
set smb-min-version [smbv1|smbv2|...]
set smb-max-version [smbv1|smbv2|...]
set use-sdwan [enable|disable]
set prefer-ipv6-dns [enable|disable]
set clipboard [enable|disable]
set host-check [none|av|...]
set host-check-interval {integer}
```

```

set host-check-policy <name1>, <name2>, ...
set limit-user-logins [enable|disable]
set mac-addr-check [enable|disable]
set mac-addr-action [allow|deny]
config mac-addr-check-rule
    Description: Client MAC address check rule.
    edit <name>
        set mac-addr-mask {integer}
        set mac-addr-list <addr1>, <addr2>, ...
    next
end
set os-check [enable|disable]
config os-check-list
    Description: SSL-VPN OS checks.
    edit <name>
        set action [deny|allow|...]
        set tolerance {integer}
        set latest-patch-level {user}
    next
end
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 skip-check-for-unsupported-os [enable|disable]
set skip-check-for-browser [enable|disable]
set hide-sso-credential [enable|disable]
config split-dns
    Description: Split DNS for SSL-VPN.
    edit <id>
        set domains {var-string}
        set dns-server1 {ipv4-address}
        set dns-server2 {ipv4-address}
        set ipv6-dns-server1 {ipv6-address}
        set ipv6-dns-server2 {ipv6-address}
    next
end
next
end

```

config vpn ssl web portal

Parameter	Description	Type	Size	Default
tunnel-mode	Enable/disable IPv4 SSL-VPN tunnel mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
ip-mode	Method by which users of this SSL-VPN tunnel obtain IP addresses.	option	-	range
	Option	Description		
	<i>range</i>	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.		
	<i>user-group</i>	Use IP the addresses associated with individual users or user groups (usually from external auth servers).		
auto-connect	Enable/disable automatic connect by client when system is up.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
keep-alive	Enable/disable automatic reconnect for FortiClient connections.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
save-password	Enable/disable FortiClient saving the user's password.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ip-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string		Maximum length: 79
exclusive-routing	Enable/disable all traffic go through tunnel only.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
service-restriction	Enable/disable tunnel service restriction.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
split-tunneling	Enable/disable IPv4 split tunneling.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
split-tunneling-routing-negate	Enable to negate split tunneling routing address.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
split-tunneling-routing-address <name>	IPv4 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79	
dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-suffix	DNS suffix.	var-string	Maximum length: 253	
wins-server1	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv6-tunnel-mode	Enable/disable IPv6 SSL-VPN tunnel mode.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ipv6-pools <name>	IPv6 firewall source address objects reserved for SSL-VPN tunnel mode clients.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
	Address name.									
ipv6-exclusive-routing	Enable/disable all IPv6 traffic go through tunnel only.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-service-restriction	Enable/disable IPv6 tunnel service restriction.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-split-tunneling	Enable/disable IPv6 split tunneling.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-split-tunneling-routing-negate	Enable to negate IPv6 split tunneling routing address.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ipv6-split-tunneling-routing-address <name>	IPv6 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79							
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::						
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::						
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::						

Parameter	Description	Type	Size	Default
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::
web-mode	Enable/disable SSL-VPN web mode.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
allow-user-access	Allow user access to SSL-VPN applications.	option	-	web ftp smb sftp telnet ssh vnc rdp ping
	Option	Description		
	web	HTTP/HTTPS access.		
	ftp	FTP access.		
	smb	SMB/CIFS access.		
	sftp	SFTP access.		
	telnet	TELNET access.		
	ssh	SSH access.		
	vnc	VNC access.		
	rdp	RDP access.		
	ping	PING access.		

Parameter	Description	Type	Size	Default						
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
display-connection-tools	Enable to display the web portal connection tools widget.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
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	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
display-status	Enable to display the web portal status widget.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
rewrite-ip-uri-ui	Rewrite contents for URI contains IP and "/ui/".	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable contents rewrite for URI contains "IP-address/ui/".</td></tr> <tr> <td><i>disable</i></td><td>Disable contents rewrite for URI contains "IP-address/ui/".</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable contents rewrite for URI contains "IP-address/ui/".	<i>disable</i>	Disable contents rewrite for URI contains "IP-address/ui/".			
Option	Description									
<i>enable</i>	Enable contents rewrite for URI contains "IP-address/ui/".									
<i>disable</i>	Disable contents rewrite for URI contains "IP-address/ui/".									
heading	Web portal heading message.	string	Maximum length: 31	SSL-VPN Portal						
redir-url	Client login redirect URL.	var-string	Maximum length: 255							
theme	Web portal color scheme.	option	-	neutrino						

Parameter	Description	Type	Size	Default
	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>dark-matter</i>	Dark Matter theme.		
	<i>onyx</i>	Onyx theme.		
	<i>eclipse</i>	Eclipse theme.		
custom-lang	Change the web portal display language. Overrides config system global set language. You can use config system custom-language and execute system custom-language to add custom language files.	string	Maximum length: 35	
smb-ntlmv1-auth	Enable support of NTLMv1 for Samba authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
smbv1	smbv1	option	-	disable
	Option	Description		
	<i>enable</i>	enable		
	<i>disable</i>	disable		
smb-min-version	SMB minimum client protocol version.	option	-	smbv2
	Option	Description		
	<i>smbv1</i>	SMB version 1.		
	<i>smbv2</i>	SMB version 2.		
	<i>smbv3</i>	SMB version 3.		
smb-max-version	SMB maximum client protocol version.	option	-	smbv3

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>smbv1</i>	SMB version 1.		
	<i>smbv2</i>	SMB version 2.		
	<i>smbv3</i>	SMB version 3.		
use-sdwan	Use SD-WAN rules to get output interface.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
prefer-ipv6-dns	prefer to query IPv6 dns first if enabled.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
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.		
host-check	Type of host checking performed on endpoints.	option	-	none
	Option	Description		
	<i>none</i>	No host checking.		
	<i>av</i>	AntiVirus software recognized by the Windows Security Center.		
	<i>fw</i>	Firewall software recognized by the Windows Security Center.		
	<i>av-fw</i>	AntiVirus and firewall software recognized by the Windows Security Center.		
	<i>custom</i>	Custom.		
host-check-interval	Periodic host check interval. Value of 0 means disabled and host checking only happens when the endpoint connects.	integer	Minimum value: 120 Maximum value: 259200	0
host-check-policy <name>	One or more policies to require the endpoint to have specific security software.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
	Host check software list name.									
limit-user-logins	Enable to limit each user to one SSL-VPN session at a time.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
mac-addr-check	Enable/disable MAC address host checking.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
mac-addr-action	Client MAC address action.	option	-	allow						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>allow</i></td><td>Allow connection when client MAC address is matched.</td></tr> <tr> <td><i>deny</i></td><td>Deny connection when client MAC address is matched.</td></tr> </tbody> </table>	Option	Description	<i>allow</i>	Allow connection when client MAC address is matched.	<i>deny</i>	Deny connection when client MAC address is matched.			
Option	Description									
<i>allow</i>	Allow connection when client MAC address is matched.									
<i>deny</i>	Deny connection when client MAC address is matched.									
os-check	Enable to let the FortiGate decide action based on client OS.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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	Enable/disable download option for FortiClient.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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						

Parameter	Description	Type	Size	Default
	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
	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	
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023	
skip-check-for-unsupported-os	Enable to skip host check if client OS does not support it.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
skip-check-for-browser	Enable to skip host check for browser support.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
hide-sso-credential	Enable to prevent SSO credential being sent to client.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web
	Option	Description		
	<i>ftp</i>	FTP.		
	<i>rdp</i>	RDP.		
	<i>sftp</i>	SFTP.		
	<i>smb</i>	SMB/CIFS.		
	<i>ssh</i>	SSH.		
	<i>telnet</i>	Telnet.		
	<i>vnc</i>	VNC.		
	<i>web</i>	HTTP/HTTPS.		
url	URL parameter.	var-string	Maximum length: 128	
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us
	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).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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>	Finish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgian.		
	<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>ko</i>	Korean.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lv-std</i>	Latvian (Standard).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>lav-leg</i>	Latvian (Legacy).		
	<i>mk</i>	Macedonian (FYROM).		
	<i>mk-std</i>	Macedonia (FYROM) - Standard.		
	<i>no</i>	Norwegian.		
	<i>no-sami</i>	Norwegian with Sami.		
	<i>pol-214</i>	Polish (214).		
	<i>pol-pr</i>	Polish (Programmers).		
	<i>pt</i>	Portuguese.		
	<i>pt-br</i>	Portuguese (Brazilian ABNT).		
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).		
	<i>ru</i>	Russian.		
	<i>ru-mne</i>	Russian - Mnemonic.		
	<i>ru-t</i>	Russian (Typewriter).		
	<i>sl</i>	Slovenian.		
	<i>sv</i>	Swedish.		
	<i>sv-sami</i>	Swedish with Sami.		
	<i>tuk</i>	Turkmen.		
	<i>tur-f</i>	Turkish F.		
	<i>tur-q</i>	Turkish Q.		
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.		
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.		
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).		
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.		
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.		
security	Security mode for RDP connection.	option	-	rdp
	Option	Description		
	<i>rdp</i>	Standard RDP encryption.		
	<i>nla</i>	Network Level Authentication.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tls</i>	TLS encryption.		
	<i>any</i>	Allow the server to choose the type of security.		
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	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 .	integer	Minimum value: 0 Maximum value: 4294967295	0
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511	
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
	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
	Option	Description		
	<i>32</i>	32bits per pixel.		
	<i>16</i>	16bits per pixel.		
	<i>8</i>	8bits per pixel.		

Parameter	Description	Type	Size	Default
sso	Single Sign-On.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SSO.		
	<i>static</i>	Static SSO.		
	<i>auto</i>	Auto SSO.		
sso-credential	Single sign-on credentials.	option	-	sslvpn-login
	Option	Description		
	<i>sslvpn-login</i>	SSL-VPN login.		
	<i>alternative</i>	Alternative.		
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable
	Option	Description		
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.		
	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.		

config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

config mac-addr-check-rule

Parameter	Description	Type	Size	Default
mac-addr-mask	Client MAC address mask.	integer	Minimum value: 1 Maximum value: 48	48
mac-addr-list <addr>	Client MAC address list. Client MAC address.	mac-address	Not Specified	

config os-check-list

Parameter	Description	Type	Size	Default
action	OS check options.	option	-	allow
	Option	Description		
	<i>deny</i>	Deny all OS versions.		
	<i>allow</i>	Allow any OS version.		
	<i>check-up-to-date</i>	Verify OS is up-to-date.		
tolerance	OS patch level tolerance.	integer	Minimum value: 0 Maximum value: 65535	0
latest-patch-level	Latest OS patch level.	user	Not Specified	0

config split-dns

Parameter	Description	Type	Size	Default
domains	Split DNS domains used for SSL-VPN clients separated by comma(,).	var-string	Maximum length: 1024	
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
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::

config vpn ssl web user-group-bookmark

Configure SSL-VPN user group bookmark.

```
config vpn ssl web user-group-bookmark
  Description: Configure SSL-VPN user group bookmark.
  edit <name>
    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 additional-params {var-string}
set description {var-string}
set keyboard-layout [ar-101|ar-102|...]
set security [rdp|nla|...]
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|static|...]
config form-data
    Description: Form data.
    edit <name>
        set value {var-string}
    next
end
set sso-credential [sslvpn-login|alternative]
set sso-username {var-string}
set sso-password {password}
set sso-credential-sent-once [enable|disable]
next
end
next
end

```

config bookmarks

Parameter	Description	Type	Size	Default
apptype	Application type.	option	-	web
Option Description				
<i>ftp</i>	FTP.			
<i>rdp</i>	RDP.			
<i>sftp</i>	SFTP.			
<i>smb</i>	SMB/CIFS.			
<i>ssh</i>	SSH.			
<i>telnet</i>	Telnet.			
<i>vnc</i>	VNC.			
<i>web</i>	HTTP/HTTPS.			

Parameter	Description	Type	Size	Default
url	URL parameter.	var-string	Maximum length: 128	
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us
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.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>fi</i>	Finish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgian.		
	<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>ko</i>	Korean.		
	<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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ru-t</i>	Russian (Typewriter).		
	<i>sl</i>	Slovenian.		
	<i>sv</i>	Swedish.		
	<i>sv-sami</i>	Swedish with Sami.		
	<i>tuk</i>	Turkmen.		
	<i>tur-f</i>	Turkish F.		
	<i>tur-q</i>	Turkish Q.		
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.		
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.		
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).		
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.		
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.		
security	Security mode for RDP connection.	option	-	rdp
	Option	Description		
	<i>rdp</i>	Standard RDP encryption.		
	<i>nla</i>	Network Level Authentication.		
	<i>tls</i>	TLS encryption.		
	<i>any</i>	Allow the server to choose the type of security.		
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	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 .	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
	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
	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
	Option	Description		
	<i>disable</i>	Disable SSO.		
	<i>static</i>	Static SSO.		
	<i>auto</i>	Auto SSO.		
sso-credential	Single sign-on credentials.	option	-	sslvpn-login
	Option	Description		
	<i>sslvpn-login</i>	SSL-VPN login.		
	<i>alternative</i>	Alternative.		
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	

Parameter	Description	Type	Size	Default
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable
	Option	Description		
	enable	Single sign-on credentials are only sent once to remote server.		
	disable	Single sign-on credentials are sent to remote server for every HTTP request.		

config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

config vpn ssl web user-bookmark

Configure SSL-VPN user bookmark.

```
config vpn ssl web user-bookmark
  Description: Configure SSL-VPN user bookmark.
  edit <name>
    set custom-lang {string}
    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 additional-params {var-string}
        set description {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set security [rdp|nla|...]
        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|static|...]
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
        next
```

```

        end
        set sso-credential [sslvpn-login|alternative]
        set sso-username {var-string}
        set sso-password {password}
        set sso-credential-sent-once [enable|disable]
    next
end
next
end

```

config vpn ssl web user-bookmark

Parameter	Description	Type	Size	Default
custom-lang	Personal language.	string	Maximum length: 35	

config bookmarks

Parameter	Description		Type	Size	Default
apptype	Application type.		option	-	web
Option					
	<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	
folder	Network shared file folder parameter.		var-string	Maximum length: 128	
domain	Login domain.		var-string	Maximum length: 128	
additional-params	Additional parameters.		var-string	Maximum length: 128	

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us
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>	Finish.			
<i>fi-sami</i>	Finnish with Sami.			
<i>fr</i>	French.			
<i>fr-ca</i>	French, Canada.			
<i>fr-ch</i>	French, Switzerland.			
<i>fr-be</i>	French, Belgian.			
<i>hr</i>	Croatian.			
<i>hu</i>	Hungarian.			

Parameter	Description	Type	Size	Default
	Option	Description		
<i>hu-101</i>	Hungarian 101-Key.			
<i>it</i>	Italian.			
<i>it-142</i>	Italian (142).			
<i>ja</i>	Japanese.			
<i>ko</i>	Korean.			
<i>lt</i>	Lithuanian.			
<i>lt-ibm</i>	Lithuanian IBM.			
<i>lt-std</i>	Lithuanian Standard.			
<i>lav-std</i>	Latvian (Standard).			
<i>lav-leg</i>	Latvian (Legacy).			
<i>mk</i>	Macedonian (FYROM).			
<i>mk-std</i>	Macedonia (FYROM) - Standard.			
<i>no</i>	Norwegian.			
<i>no-sami</i>	Norwegian with Sami.			
<i>pol-214</i>	Polish (214).			
<i>pol-pr</i>	Polish (Programmers).			
<i>pt</i>	Portuguese.			
<i>pt-br</i>	Portuguese (Brazilian ABNT).			
<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).			
<i>ru</i>	Russian.			
<i>ru-mne</i>	Russian - Mnemonic.			
<i>ru-t</i>	Russian (Typewriter).			
<i>sl</i>	Slovenian.			
<i>sv</i>	Swedish.			
<i>sv-sami</i>	Swedish with Sami.			
<i>tuk</i>	Turkmen.			
<i>tur-f</i>	Turkish F.			
<i>tur-q</i>	Turkish Q.			
<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<code>zh-sym-us</code>	Chinese (Simplified) - US Keyboard.		
	<code>zh-tr-hk</code>	Chinese (Traditional, Hong Kong S.A.R.).		
	<code>zh-tr-mo</code>	Chinese (Traditional Macao S.A.R.) - US Keyboard.		
	<code>zh-tr-us</code>	Chinese (Traditional) - US keyboard.		
security	Security mode for RDP connection.	option	-	rdp
	Option	Description		
	<code>rdp</code>	Standard RDP encryption.		
	<code>nla</code>	Network Level Authentication.		
	<code>tls</code>	TLS encryption.		
	<code>any</code>	Allow the server to choose the type of security.		
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	Option	Description		
	<code>enable</code>	Enable sending of preconnection ID.		
	<code>disable</code>	Disable sending of preconnection ID.		
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 4294967295	0
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511	
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
	Option	Description		
	<code>enable</code>	Enable restricted admin mode for RDP.		
	<code>disable</code>	Disable restricted admin mode for RDP.		

Parameter	Description	Type	Size	Default
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
		Option	Description	
		32	32bits per pixel.	
		16	16bits per pixel.	
		8	8bits per pixel.	
sso	Single Sign-On.	option	-	disable
		Option	Description	
		disable	Disable SSO.	
		static	Static SSO.	
		auto	Auto SSO.	
sso-credential	Single sign-on credentials.	option	-	sslvpn-login
		Option	Description	
		sslvpn-login	SSL-VPN login.	
		alternative	Alternative.	
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable
		Option	Description	
		enable	Single sign-on credentials are only sent once to remote server.	
		disable	Single sign-on credentials are sent to remote server for every HTTP request.	

config form-data

Parameter	Description	Type	Size	Default
value	Value.	var-string	Maximum length: 63	

config vpn ssl settings

Configure SSL-VPN.

```
config vpn ssl settings
    Description: Configure SSL-VPN.
    set status [enable|disable]
    set reqclientcert [enable|disable]
    set user-peer {string}
    set ssl-maxproto-ver [tls1-0|tls1-1|...]
    set ssl-minproto-ver [tls1-0|tls1-1|...]
    set banned-cipher {option1}, {option2}, ...
    set ciphersuite {option1}, {option2}, ...
    set ssl-insert-empty-fragment [enable|disable]
    set https-redirect [enable|disable]
    set x-content-type-options [enable|disable]
    set ssl-client-renegotiation [disable|enable]
    set force-two-factor-auth [enable|disable]
    set unsafe-legacy-renegotiation [enable|disable]
    set servercert {string}
    set algorithm [high|medium|...]
    set idle-timeout {integer}
    set auth-timeout {integer}
    set login-attempt-limit {integer}
    set login-block-time {integer}
    set login-timeout {integer}
    set dtls-hello-timeout {integer}
    set tunnel-ip-pools <name1>, <name2>, ...
    set tunnel-ipv6-pools <name1>, <name2>, ...
    set dns-suffix {var-string}
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
    set ipv6-dns-server1 {ipv6-address}
    set ipv6-dns-server2 {ipv6-address}
    set ipv6-wins-server1 {ipv6-address}
    set ipv6-wins-server2 {ipv6-address}
    set url-obscuration [enable|disable]
    set http-compression [enable|disable]
    set http-only-cookie [enable|disable]
    set deflate-compression-level {integer}
    set deflate-min-data-size {integer}
    set port {integer}
    set port-precedence [enable|disable]
    set auto-tunnel-static-route [enable|disable]
    set header-x-forwarded-for [pass|add|...]
    set source-interface <name1>, <name2>, ...
```

```

set source-address <name1>, <name2>, ...
set source-address-negate [enable|disable]
set source-address6 <name1>, <name2>, ...
set source-address6-negate [enable|disable]
set default-portal {string}
config authentication-rule
    Description: Authentication rule for SSL-VPN.
    edit <id>
        set source-interface <name1>, <name2>, ...
        set source-address <name1>, <name2>, ...
        set source-address-negate [enable|disable]
        set source-address6 <name1>, <name2>, ...
        set source-address6-negate [enable|disable]
        set users <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set portal {string}
        set realm {string}
        set client-cert [enable|disable]
        set user-peer {string}
        set cipher [any|high|...]
        set auth [any|local|...]
    next
end
set dtls-tunnel [enable|disable]
set dtls-max Proto-ver [dtls1-0|dtls1-2]
set dtls-min Proto-ver [dtls1-0|dtls1-2]
set check-referer [enable|disable]
set http-request-header-timeout {integer}
set http-request-body-timeout {integer}
set auth-session-check-source-ip [enable|disable]
set tunnel-connect-without-reauth [enable|disable]
set tunnel-user-session-timeout {integer}
set hsts-include-subdomains [enable|disable]
set transform-backward-slashes [enable|disable]
set encode-2f-sequence [enable|disable]
set encrypt-and-store-password [enable|disable]
set client-sigalgs [no-rsa-pss|all]
set dual-stack-mode [enable|disable]
set tunnel-addr-assigned-method [first-available|round-robin]
    set saml-redirect-port {integer}
end

```

config vpn ssl settings

Parameter	Description	Type	Size	Default
status	Enable/disable SSL-VPN.	option	-	enable
Parameter	Description	Type	Size	Default
Option	Description			
<i>enable</i>	Enable SSL-VPN.			
<i>disable</i>	Disable SSL-VPN.			

Parameter	Description	Type	Size	Default
reqclientcert	Enable/disable to require client certificates for all SSL-VPN users.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
user-peer	Name of user peer.	string	Maximum length: 35	
ssl-max-proto-ver	SSL maximum protocol version.	option	-	tls1-3
	Option	Description		
	<i>tls1-0</i>	TLS version 1.0.		
	<i>tls1-1</i>	TLS version 1.1.		
	<i>tls1-2</i>	TLS version 1.2.		
	<i>tls1-3</i>	TLS version 1.3.		
ssl-min-proto-ver	SSL minimum protocol version.	option	-	tls1-2
	Option	Description		
	<i>tls1-0</i>	TLS version 1.0.		
	<i>tls1-1</i>	TLS version 1.1.		
	<i>tls1-2</i>	TLS version 1.2.		
	<i>tls1-3</i>	TLS version 1.3.		
banned-cipher	Select one or more cipher technologies that cannot be used in SSL-VPN negotiations. Only applies to TLS 1.2 and below.	option	-	
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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 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.		
ciphersuite	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, set ssl-maxproto-ver to tls1-2 or below.	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.		
	<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.		

Parameter	Description	Type	Size	Default
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
https-redirect	Enable/disable redirect of port 80 to SSL-VPN port.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ssl-client-renegotiation	Enable/disable to allow client renegotiation by the server if the tunnel goes down.	option	-	disable
	Option	Description		
	<i>disable</i>	Abort any SSL connection that attempts to renegotiate.		
	<i>enable</i>	Allow a SSL client to renegotiate.		
force-two-factor-auth	Enable/disable only PKI users with two-factor authentication for SSL-VPNs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
servercert	Name of the server certificate to be used for SSL-VPNs.	string	Maximum length: 35	Fortinet_Factory **
algorithm	Force the SSL-VPN security level. High allows only high. Medium allows medium and high. Low allows any.	option	-	high
	Option	Description		
	<i>high</i>	High algorithms.		
	<i>medium</i>	High and medium algorithms.		
	<i>default</i>	default		
	<i>low</i>	All algorithms.		
idle-timeout	SSL-VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200	300
auth-timeout	SSL-VPN authentication timeout .	integer	Minimum value: 0 Maximum value: 259200	28800
login-attempt-limit	SSL-VPN maximum login attempt times before block .	integer	Minimum value: 0 Maximum value: 4294967295	2
login-block-time	Time for which a user is blocked from logging in after too many failed login attempts .	integer	Minimum value: 0 Maximum value: 4294967295	60
login-timeout	SSLVPN maximum login timeout .	integer	Minimum value: 10 Maximum value: 180	30

Parameter	Description	Type	Size	Default
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout .	integer	Minimum value: 10 Maximum value: 60	10
tunnel-ip-pools <name>	Names of the IPv4 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79	
tunnel-ipv6-pools <name>	Names of the IPv6 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79	
dns-suffix	DNS suffix used for SSL-VPN clients.	var-string	Maximum length: 253	
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
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
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::
url-obscuration	Enable/disable to obscure the host name of the URL of the web browser display.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			
http-compression	Enable/disable to allow HTTP compression over SSL-VPN tunnels.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
http-only-cookie	Enable/disable SSL-VPN support for HttpOnly cookies.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
deflate-compression-level	Compression level (0~9).	integer	Minimum value: 0 Maximum value: 9	6
deflate-min-data-size	Minimum amount of data that triggers compression .	integer	Minimum value: 200 Maximum value: 65535	300
port	SSL-VPN access port .	integer	Minimum value: 1 Maximum value: 65535	10443
port-precedence	Enable/disable, Enable means that if SSL-VPN connections are allowed on an interface admin GUI connections are blocked on that interface.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
auto-tunnel-static-route	Enable/disable to auto-create static routes for the SSL-VPN tunnel IP addresses.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-	add

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.		
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79	
source-address-negate	Enable/disable negated source address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79	
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
default-portal	Default SSL-VPN portal.	string	Maximum length: 35	
dtls-tunnel	Enable/disable DTLS to prevent eavesdropping, tampering, or message forgery.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dtls-max-proto-ver	DTLS maximum protocol version.	option	-	dtls1-2

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dtls1-0</i>	DTLS version 1.0.		
	<i>dtls1-2</i>	DTLS version 1.2.		
dtls-min-proto-ver	DTLS minimum protocol version.	option	-	dtls1-0
	Option	Description		
	<i>dtls1-0</i>	DTLS version 1.0.		
	<i>dtls1-2</i>	DTLS version 1.2.		
check-referer	Enable/disable verification of referer field in HTTP request header.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable verification of referer field in HTTP request header.		
	<i>disable</i>	Disable verification of referer field in HTTP request header.		
http-request-header-timeout	SSL-VPN session is disconnected if an HTTP request header is not received within this time .	integer	Minimum value: 0 Maximum value: 4294967295	20
http-request-body-timeout	SSL-VPN session is disconnected if an HTTP request body is not received within this time .	integer	Minimum value: 0 Maximum value: 4294967295	30
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable checking of source IP for authentication session.		
	<i>disable</i>	Disable checking of source IP for authentication session.		
tunnel-connect-without-reauth	Enable/disable tunnel connection without re-authorization if previous connection dropped.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable tunnel connection without re-authorization.		
	<i>disable</i>	Disable tunnel connection without re-authorization.		

Parameter	Description	Type	Size	Default						
tunnel-user-session-timeout	Time out value to clean up user session after tunnel connection is dropped .	integer	Minimum value: 1 Maximum value: 255	30						
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
encode-2f-sequence	Encode \2F sequence to forward slash in URLs.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
encrypt-and-store-password	Encrypt and store user passwords for SSL-VPN web sessions.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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-sigalgs	Set signature algorithms related to client authentication. Affects TLS version <= 1.2 only.	option	-	all						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>no-rsa-pss</i></td><td>Disable RSA-PSS signature algorithms for client authentication.</td></tr> <tr> <td><i>all</i></td><td>Enable all supported signature algorithms for client authentication.</td></tr> </tbody> </table>	Option	Description	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.	<i>all</i>	Enable all supported signature algorithms for client authentication.			
Option	Description									
<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.									
<i>all</i>	Enable all supported signature algorithms for client authentication.									

Parameter	Description	Type	Size	Default
dual-stack-mode	Tunnel mode: enable parallel IPv4 and IPv6 tunnel. Web mode: support IPv4 and IPv6 bookmarks in the portal.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
tunnel-addr-assigned-method	Method used for assigning address for tunnel.	option	-	first-available
	Option	Description		
	first-available	Assign the first available address from the pools.		
	round-robin	Assign the available address from the pool with a round robin fashion.		
saml-redirect-port	SAML local redirect port in the machine running FCT . 0 is to disable redirection on FGT side.	integer	Minimum value: 0 Maximum value: 65535	8020

** Values may differ between models.

config authentication-rule

Parameter	Description	Type	Size	Default
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default								
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
users <name>	User name. User name.	string	Maximum length: 79									
groups <name>	User groups. Group name.	string	Maximum length: 79									
portal	SSL-VPN portal.	string	Maximum length: 35									
realm	SSL-VPN realm.	string	Maximum length: 35									
client-cert	Enable/disable SSL-VPN client certificate restrictive.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
user-peer	Name of user peer.	string	Maximum length: 35									
cipher	SSL-VPN cipher strength.	option	-	high								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>any</i></td><td>Any cipher strength.</td></tr> <tr> <td><i>high</i></td><td>High cipher strength (>= 168 bits).</td></tr> <tr> <td><i>medium</i></td><td>Medium cipher strength (>= 128 bits).</td></tr> </tbody> </table>	Option	Description	<i>any</i>	Any cipher strength.	<i>high</i>	High cipher strength (>= 168 bits).	<i>medium</i>	Medium cipher strength (>= 128 bits).			
Option	Description											
<i>any</i>	Any cipher strength.											
<i>high</i>	High cipher strength (>= 168 bits).											
<i>medium</i>	Medium cipher strength (>= 128 bits).											
auth	SSL-VPN authentication method restriction.	option	-	any								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>any</i></td><td>Any</td></tr> <tr> <td><i>local</i></td><td>Local</td></tr> <tr> <td><i>radius</i></td><td>RADIUS</td></tr> </tbody> </table>	Option	Description	<i>any</i>	Any	<i>local</i>	Local	<i>radius</i>	RADIUS			
Option	Description											
<i>any</i>	Any											
<i>local</i>	Local											
<i>radius</i>	RADIUS											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tacacs+</i>	TACACS+		
	<i>ldap</i>	LDAP		
	<i>peer</i>	PEER		

config vpn ssl client

```

client
config vpn ssl client
  Description: client
  edit <name>
    set comment {var-string}
    set interface {string}
    set user {string}
    set psk {password-3}
    set peer {string}
    set server {string}
    set port {integer}
    set realm {string}
    set status [enable|disable]
    set certificate {string}
    set source-ip {string}
    set distance {integer}
    set priority {integer}
  next
end

```

config vpn ssl client

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
interface	SSL interface to send/receive traffic over.	string	Maximum length: 15	
user	Username to offer to the peer to authenticate the client.	string	Maximum length: 35	
psk	Pre-shared secret to authenticate with the server (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
peer	Authenticate peer's certificate with the peer/peergrp.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
server	IPv4, IPv6 or DNS address of the SSL-VPN server.	string	Maximum length: 63	
port	SSL-VPN server port.	integer	Minimum value: 1 Maximum value: 65535	443
realm	Realm name configured on SSL-VPN server.	string	Maximum length: 35	
status	Enable/disable this SSL-VPN client configuration.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the SSL-VPN configuration.		
	<i>disable</i>	Disable the SSL-VPN configuration.		
certificate	Certificate to offer to SSL-VPN server if it requests one.	string	Maximum length: 35	
source-ip	IPv4 or IPv6 address to use as a source for the SSL-VPN connection to the server.	string	Maximum length: 63	
distance	Distance for routes added by SSL-VPN .	integer	Minimum value: 1 Maximum value: 255	10
priority	Priority for routes added by SSL-VPN .	integer	Minimum value: 0 Maximum value: 4294967295	0

config vpn ssl monitor

SSL-VPN session.

```
config vpn ssl monitor
    Description: SSL-VPN session.
end
```

config vpn ipsec phase1

Configure VPN remote gateway.

```
config vpn ipsec phase1
    Description: Configure VPN remote gateway.
    edit <name>
        set type [static|dynamic|...]
```

```

set interface {string}
set ike-version [1|2]
set remote-gw {ipv4-address}
set local-gw {ipv4-address}
set remotegw-ddns {string}
set keylife {integer}
set certificate <name1>, <name2>, ...
set authmethod [psk|signature]
set authmethod-remote [psk|signature]
set mode [aggressive|main]
set peertype [any|one|...]
set peerid {string}
set usrrgp {string}
set peer {string}
set peergrp {string}
set mode-cfg [disable|enable]
set assign-ip [disable|enable]
set assign-ip-from [range|usrrgp|...]
set ipv4-start-ip {ipv4-address}
set ipv4-end-ip {ipv4-address}
set ipv4-netmask {ipv4-netmask}
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dns-mode [manual|auto]
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
set ipv4-split-include {string}
set split-include-service {string}
set ipv4-name {string}
set ipv6-start-ip {ipv6-address}
set ipv6-end-ip {ipv6-address}
set ipv6-prefix {integer}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set ipv6-split-include {string}
set ipv6-name {string}
set ip-delay-interval {integer}
set unity-support [disable|enable]
set domain {string}

```

```
set banner {var-string}
set include-local-lan [disable|enable]
set ipv4-split-exclude {string}
set ipv6-split-exclude {string}
set save-password [disable|enable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set backup-gateway <address1>, <address2>, ...
set proposal {option1}, {option2}, ...
set add-route [disable|enable]
set add-gw-route [enable|disable]
set psksecret {password-3}
set psksecret-remote {password-3}
set keepalive {integer}
set distance {integer}
set priority {integer}
set localid {string}
set localid-type [auto|fqdn|...]
set auto-negotiate [enable|disable]
set negotiate-timeout {integer}
set fragmentation [enable|disable]
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set forticlient-enforcement [enable|disable]
set comments {var-string}
set npu-offload [enable|disable]
set send-cert-chain [enable|disable]
set dhgrp {option1}, {option2}, ...
set suite-b [disable|suite-b-gcm-128|...]
set eap [enable|disable]
set eap-identity [use-id-payload|send-request]
set eap-exclude-peergrp {string}
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 authusrgroup {string}
set mesh-selector-type [disable|subnet|...]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ha-sync-esp-seqno [enable|disable]
set natraversal [enable|disable|...]
set esn [require|allow|...]
set fragmentation-mtu {integer}
set childless-ike [enable|disable]
set rekey [enable|disable]
set digital-signature-auth [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set rsa-signature-format [pkcs1|pss]
```

```

set enforce-unique-id [disable|keep-new|...]
set cert-id-validation [enable|disable]
set fec-egress [enable|disable]
set fec-send-timeout {integer}
set fec-base {integer}
set fec-codec {integer}
set fec-redundant {integer}
set fec-ingress [enable|disable]
set fec-receive-timeout {integer}
set network-overlay [disable|enable]
set network-id {integer}
set loopback-asymroute [enable|disable]
next
end

```

config vpn ipsec phase1

Parameter	Description	Type	Size	Default
type	Remote gateway type.	option	-	static
	Option	Description		
	static	Remote VPN gateway has fixed IP address.		
	dynamic	Remote VPN gateway has dynamic IP address.		
	ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.		
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35	
ike-version	IKE protocol version.	option	-	1
	Option	Description		
	1	Use IKEv1 protocol.		
	2	Use IKEv2 protocol.		
remote-gw	Remote VPN gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	Local VPN gateway.	ipv4-address	Not Specified	0.0.0.0
remotegw-ddns	Domain name of remote gateway (eg. name.DDNS.com).	string	Maximum length: 63	
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400
certificate <name>	Names of up to 4 signed personal certificates.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default												
	Certificate name.															
authmethod	Authentication method.	option	-	psk												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>psk</i></td><td>PSK authentication method.</td></tr> <tr> <td><i>signature</i></td><td>Signature authentication method.</td></tr> </tbody> </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.															
authmethod-remote	Authentication method (remote side).	option	-													
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>psk</i></td><td>PSK authentication method.</td></tr> <tr> <td><i>signature</i></td><td>Signature authentication method.</td></tr> </tbody> </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	ID protection mode used to establish a secure channel.	option	-	main												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>aggressive</i></td><td>Aggressive mode.</td></tr> <tr> <td><i>main</i></td><td>Main mode.</td></tr> </tbody> </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	-	peer												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>any</i></td><td>Accept any peer ID.</td></tr> <tr> <td><i>one</i></td><td>Accept this peer ID.</td></tr> <tr> <td><i>dialup</i></td><td>Accept peer ID in dialup group.</td></tr> <tr> <td><i>peer</i></td><td>Accept this peer certificate.</td></tr> <tr> <td><i>peergrp</i></td><td>Accept this peer certificate group.</td></tr> </tbody> </table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.			
Option	Description															
<i>any</i>	Accept any peer ID.															
<i>one</i>	Accept this peer ID.															
<i>dialup</i>	Accept peer ID in dialup group.															
<i>peer</i>	Accept this peer certificate.															
<i>peergrp</i>	Accept this peer certificate group.															
peerid	Accept this peer identity.	string	Maximum length: 255													
usrgrp	User group name for dialup peers.	string	Maximum length: 35													
peer	Accept this peer certificate.	string	Maximum length: 35													
peergrp	Accept this peer certificate group.	string	Maximum length: 35													
mode-cfg	Enable/disable configuration method.	option	-	disable												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable Configuration Method.		
	<i>enable</i>	Enable Configuration Method.		
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not assign an IP address to the IPsec interface.		
	<i>enable</i>	Assign an IP address to the IPsec interface.		
assign-ip-from	Method by which the IP address will be assigned.	option	-	range
	Option	Description		
	<i>range</i>	Assign IP address from locally defined range.		
	<i>usrgrp</i>	Assign IP address via user group.		
	<i>dhcp</i>	Assign IP address via DHCP.		
	<i>name</i>	Assign IP address from firewall address or group.		
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::
dns-mode	DNS server mode.	option	-	manual
	Option	Description		
	<i>manual</i>	Manually configure DNS servers.		
	<i>auto</i>	Use default DNS servers.		
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79	
split-include-service	Split-include services.	string	Maximum length: 79	
ipv4-name	IPv4 address name.	string	Maximum length: 79	
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79	
ipv6-name	IPv6 address name.	string	Maximum length: 79	
ip-delay-interval	IP address reuse delay interval in seconds .	integer	Minimum value: 0 Maximum value: 28800	0
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable
Option	Description			
disable	Disable Cisco Unity Configuration Method Extensions.			
enable	Enable Cisco Unity Configuration Method Extensions.			
domain	Instruct unity clients about the default DNS domain.	string	Maximum length: 63	
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024	

Parameter	Description	Type	Size	Default
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable local LAN access on Unity clients.		
	<i>enable</i>	Enable local LAN access on Unity clients.		
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79	
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79	
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable saving XAuth username and password on VPN clients.		
	<i>enable</i>	Enable saving XAuth username and password on VPN clients.		
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.		
	<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.		
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.		
	<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.		
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
proposal	Phase1 proposal.	option	-	
Option	Description			
<i>des-md5</i>	des-md5			
<i>des-sha1</i>	des-sha1			
<i>des-sha256</i>	des-sha256			
<i>des-sha384</i>	des-sha384			
<i>des-sha512</i>	des-sha512			
<i>3des-md5</i>	3des-md5			
<i>3des-sha1</i>	3des-sha1			
<i>3des-sha256</i>	3des-sha256			
<i>3des-sha384</i>	3des-sha384			
<i>3des-sha512</i>	3des-sha512			
<i>aes128-md5</i>	aes128-md5			
<i>aes128-sha1</i>	aes128-sha1			
<i>aes128-sha256</i>	aes128-sha256			
<i>aes128-sha384</i>	aes128-sha384			
<i>aes128-sha512</i>	aes128-sha512			
<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1			
<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256			
<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384			
<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512			
<i>aes192-md5</i>	aes192-md5			
<i>aes192-sha1</i>	aes192-sha1			
<i>aes192-sha256</i>	aes192-sha256			
<i>aes192-sha384</i>	aes192-sha384			
<i>aes192-sha512</i>	aes192-sha512			
<i>aes256-md5</i>	aes256-md5			
<i>aes256-sha1</i>	aes256-sha1			
<i>aes256-sha256</i>	aes256-sha256			
<i>aes256-sha384</i>	aes256-sha384			

Parameter	Description	Type	Size	Default
Option	Description			
<code>aes256-sha512</code>	aes256-sha512			
<code>aes256gcm-prfsha1</code>	aes256gcm-prfsha1			
<code>aes256gcm-prfsha256</code>	aes256gcm-prfsha256			
<code>aes256gcm-prfsha384</code>	aes256gcm-prfsha384			
<code>aes256gcm-prfsha512</code>	aes256gcm-prfsha512			
<code>chacha20poly1305-prfsha1</code>	chacha20poly1305-prfsha1			
<code>chacha20poly1305-prfsha256</code>	chacha20poly1305-prfsha256			
<code>chacha20poly1305-prfsha384</code>	chacha20poly1305-prfsha384			
<code>chacha20poly1305-prfsha512</code>	chacha20poly1305-prfsha512			
<code>aria128-md5</code>	aria128-md5			
<code>aria128-sha1</code>	aria128-sha1			
<code>aria128-sha256</code>	aria128-sha256			
<code>aria128-sha384</code>	aria128-sha384			
<code>aria128-sha512</code>	aria128-sha512			
<code>aria192-md5</code>	aria192-md5			
<code>aria192-sha1</code>	aria192-sha1			
<code>aria192-sha256</code>	aria192-sha256			
<code>aria192-sha384</code>	aria192-sha384			
<code>aria192-sha512</code>	aria192-sha512			
<code>aria256-md5</code>	aria256-md5			
<code>aria256-sha1</code>	aria256-sha1			
<code>aria256-sha256</code>	aria256-sha256			
<code>aria256-sha384</code>	aria256-sha384			
<code>aria256-sha512</code>	aria256-sha512			
<code>seed-md5</code>	seed-md5			
<code>seed-sha1</code>	seed-sha1			
<code>seed-sha256</code>	seed-sha256			
<code>seed-sha384</code>	seed-sha384			
<code>seed-sha512</code>	seed-sha512			

Parameter	Description	Type	Size	Default
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add a route to destination of peer selector.		
	<i>enable</i>	Add route to destination of peer selector.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable
	Option	Description		
	<i>enable</i>	Automatically add a route to the remote gateway.		
	<i>disable</i>	Do not automatically add a route to the remote gateway.		
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255	15
priority	Priority for routes added by IKE .	integer	Minimum value: 0 Maximum value: 4294967295	0
localid	Local ID.	string	Maximum length: 63	
localid-type	Local ID type.	option	-	auto
	Option	Description		
	<i>auto</i>	Select ID type automatically.		
	<i>fqdn</i>	Use fully qualified domain name.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.		
	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.		
negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300	30
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.		
	<i>disable</i>	Disable intra-IKE fragmentation support.		
dpd	Dead Peer Detection mode.	option	-	on-demand
	Option	Description		
	<i>disable</i>	Disable Dead Peer Detection.		
	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.		
	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.		
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3
dpd-retryinterval	DPD retry interval.	user	Not Specified	
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FortiClient enforcement.		
	<i>disable</i>	Disable FortiClient enforcement.		
comments	Comment.	var-string	Maximum length: 255	
npu-offload *	Enable/disable offloading NPU.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sending certificate chain.		
	<i>disable</i>	Disable sending certificate chain.		
dhgrp	DH group.	option	-	14
	Option	Description		
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		
	14	DH Group 14.		
	15	DH Group 15.		
	16	DH Group 16.		
	17	DH Group 17.		
	18	DH Group 18.		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
	27	DH Group 27.		
	28	DH Group 28.		
	29	DH Group 29.		

Parameter	Description	Type	Size	Default
	Option	Description		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		
suite-b	Use Suite-B.	option	-	disable
	Option	Description		
	disable	Do not use UI suite.		
	suite-b-gcm-128	Use Suite-B-GCM-128.		
	suite-b-gcm-256	Use Suite-B-GCM-256.		
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable
	Option	Description		
	enable	Enable IKEv2 EAP authentication.		
	disable	Disable IKEv2 EAP authentication.		
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload
	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	
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable
	Option	Description		
	enable	Enable verification of RADIUS accounting record.		
	disable	Disable verification of RADIUS accounting record.		
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable
	Option	Description		
	disable	Disable use of IKEv2 Postquantum Preshared Key (PPK).		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.		
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.		
	<i>static-fortigate</i>	Site to Site - FortiGate.		
	<i>dialup-fortigate</i>	Dial Up - FortiGate.		
	<i>static-cisco</i>	Site to Site - Cisco.		
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.		
	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).		
	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.		
	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.		
xauthtype	XAuth type.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>client</i>	Enable as client.		
	<i>pap</i>	Enable as server PAP.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	Option	Description		
	<i>disable</i>	Disable IKE SA re-authentication.		
	<i>enable</i>	Enable IKE SA re-authentication.		
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
	Option	Description		
	<i>enable</i>	Enable IKEv2 IDi group authentication.		
	<i>disable</i>	Disable IKEv2 IDi group authentication.		
group-authentication-secret	Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by a leading 0x.)	password-3	Not Specified	
authusgrp	Authentication user group.	string	Maximum length: 35	
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>subnet</i>	Enable addition of matching subnet selector.		
	<i>host</i>	Enable addition of host to host selector.		
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPsec tunnel idle timeout.		
	<i>disable</i>	Disable IPsec tunnel idle timeout.		

Parameter	Description	Type	Size	Default								
idle-timeoutinterval	IPsec tunnel idle timeout in minutes .	integer	Minimum value: 5 Maximum value: 43200	15								
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable HA syncing of ESP sequence numbers.</td></tr> <tr> <td><i>disable</i></td><td>Disable HA syncing of ESP sequence numbers.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable HA syncing of ESP sequence numbers.	<i>disable</i>	Disable HA syncing of ESP sequence numbers.					
Option	Description											
<i>enable</i>	Enable HA syncing of ESP sequence numbers.											
<i>disable</i>	Disable HA syncing of ESP sequence numbers.											
nattraversal	Enable/disable NAT traversal.	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable IPsec NAT traversal.</td></tr> <tr> <td><i>disable</i></td><td>Disable IPsec NAT traversal.</td></tr> <tr> <td><i>forced</i></td><td>Force IPsec NAT traversal on.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.			
Option	Description											
<i>enable</i>	Enable IPsec NAT traversal.											
<i>disable</i>	Disable IPsec NAT traversal.											
<i>forced</i>	Force IPsec NAT traversal on.											
esn *	Extended sequence number (ESN) negotiation.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>require</i></td><td>Require extended sequence number.</td></tr> <tr> <td><i>allow</i></td><td>Allow extended sequence number.</td></tr> <tr> <td><i>disable</i></td><td>Disable extended sequence number.</td></tr> </tbody> </table>	Option	Description	<i>require</i>	Require extended sequence number.	<i>allow</i>	Allow extended sequence number.	<i>disable</i>	Disable extended sequence number.			
Option	Description											
<i>require</i>	Require extended sequence number.											
<i>allow</i>	Allow extended sequence number.											
<i>disable</i>	Disable extended sequence number.											
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000	1200								
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr> <tr> <td><i>disable</i></td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).					
Option	Description											
<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).											
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).											
rekey	Enable/disable phase1 rekey.	option	-	enable								

Parameter	Description	Type	Size	Default
	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
	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
	Option	Description		
	<i>sha1</i>	SHA1.		
	<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
	Option	Description		
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.		
	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).		
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable
	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

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
	disable	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable
	Option	Description		
	enable	Enable Forward Error Correction for egress IPsec traffic.		
	disable	Disable Forward Error Correction for egress IPsec traffic.		
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 1000	8
fec-base	Number of base Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100	20
fec-codec	ipsec fec encoding/decoding algorithm (0: reed-solomon, 1: xor).	integer	Minimum value: 0 Maximum value: 1	0
fec-redundant	Number of redundant Forward Error Correction packets (0 - 100, when fec-codec is reed-solomon or 1 when fec-codec is xor .	integer	Minimum value: 0 Maximum value: 100	1
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable
	Option	Description		
	enable	Enable Forward Error Correction for ingress IPsec traffic.		
	disable	Disable Forward Error Correction for ingress IPsec traffic.		
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 10000	5000
network-overlay	Enable/disable network overlays.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	disable	Disable network overlays.		
	enable	Enable network overlays.		
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable
	Option	Description		
	enable	Allow ingress/egress IKE traffic to be routed over different interfaces.		
	disable	Ingress/egress IKE traffic must be routed over the same interface.		

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

config ipv6-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::

config vpn ipsec phase2

Configure VPN autokey tunnel.

```
config vpn ipsec phase2
  Description: Configure VPN autokey tunnel.
  edit <name>
    set phase1name {string}
    set dhcp-ipsec [enable|disable]
```

```

set use-natip [enable|disable]
set selector-match [exact|subset|...]
set proposal {option1}, {option2}, ...
set pfs [enable|disable]
set ipv4-df [enable|disable]
set dhgrp {option1}, {option2}, ...
set replay [enable|disable]
set keepalive [enable|disable]
set auto-negotiate [enable|disable]
set add-route [phase1|enable|...]
set keylifeseconds {integer}
set keylifesecs {integer}
set keylife-type [seconds|kbs|...]
set single-source [enable|disable]
set route-overlap [use-old|use-new|...]
set encapsulation [tunnel-mode|transport-mode]
set l2tp [enable|disable]
set comments {var-string}
set initiator-ts-narrow [enable|disable]
set diffserv [enable|disable]
set diffservcode {user}
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

Parameter	Description	Type	Size	Default
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 35	
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
use-natip	Enable to use the FortiGate public IP as the source selector when outbound NAT is used.	option	-	enable
	Option	Description		
	<i>enable</i>	Replace source selector with interface IP when using outbound NAT.		
	<i>disable</i>	Do not modify source selector when using outbound NAT.		
selector-match	Match type to use when comparing selectors.	option	-	auto
	Option	Description		
	<i>exact</i>	Match selectors exactly.		
	<i>subset</i>	Match selectors by subset.		
	<i>auto</i>	Use subset or exact match depending on selector address type.		
proposal	Phase2 proposal.	option	-	
	Option	Description		
	<i>null-md5</i>	null-md5		
	<i>null-sha1</i>	null-sha1		
	<i>null-sha256</i>	null-sha256		
	<i>null-sha384</i>	null-sha384		
	<i>null-sha512</i>	null-sha512		
	<i>des-null</i>	des-null		
	<i>des-md5</i>	des-md5		
	<i>des-sha1</i>	des-sha1		
	<i>des-sha256</i>	des-sha256		
	<i>des-sha384</i>	des-sha384		
	<i>des-sha512</i>	des-sha512		
	<i>3des-null</i>	3des-null		
	<i>3des-md5</i>	3des-md5		
	<i>3des-sha1</i>	3des-sha1		

Parameter	Description	Type	Size	Default
	Option	Description		
	<code>3des-sha256</code>	3des-sha256		
	<code>3des-sha384</code>	3des-sha384		
	<code>3des-sha512</code>	3des-sha512		
	<code>aes128-null</code>	aes128-null		
	<code>aes128-md5</code>	aes128-md5		
	<code>aes128-sha1</code>	aes128-sha1		
	<code>aes128-sha256</code>	aes128-sha256		
	<code>aes128-sha384</code>	aes128-sha384		
	<code>aes128-sha512</code>	aes128-sha512		
	<code>aes128gcm</code>	aes128gcm		
	<code>aes192-null</code>	aes192-null		
	<code>aes192-md5</code>	aes192-md5		
	<code>aes192-sha1</code>	aes192-sha1		
	<code>aes192-sha256</code>	aes192-sha256		
	<code>aes192-sha384</code>	aes192-sha384		
	<code>aes192-sha512</code>	aes192-sha512		
	<code>aes256-null</code>	aes256-null		
	<code>aes256-md5</code>	aes256-md5		
	<code>aes256-sha1</code>	aes256-sha1		
	<code>aes256-sha256</code>	aes256-sha256		
	<code>aes256-sha384</code>	aes256-sha384		
	<code>aes256-sha512</code>	aes256-sha512		
	<code>aes256gcm</code>	aes256gcm		
	<code>chacha20poly1305</code>	chacha20poly1305		
	<code>aria128-null</code>	aria128-null		
	<code>aria128-md5</code>	aria128-md5		
	<code>aria128-sha1</code>	aria128-sha1		
	<code>aria128-sha256</code>	aria128-sha256		
	<code>aria128-sha384</code>	aria128-sha384		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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		
pfs	Enable/disable PFS feature.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-	disable
	Option	Description		
	<i>enable</i>	Set IPv4 DF.		
	<i>disable</i>	Reset IPv4 DF.		

Parameter	Description	Type	Size	Default
dhgrp	Phase2 DH group.	option	-	14
	Option	Description		
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		
	14	DH Group 14.		
	15	DH Group 15.		
	16	DH Group 16.		
	17	DH Group 17.		
	18	DH Group 18.		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
	27	DH Group 27.		
	28	DH Group 28.		
	29	DH Group 29.		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		
replay	Enable/disable replay detection.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
keepalive	Enable/disable keep alive.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
add-route	Enable/disable automatic route addition.	option	-	phase1
	Option	Description		
	<i>phase1</i>	Add route according to phase1 add-route setting.		
	<i>enable</i>	Add route for remote proxy ID.		
	<i>disable</i>	Do not add route for remote proxy ID.		
keylifesecs	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800	43200
keylifekbs	Phase2 key life in number of bytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295	5120
keylife-type	Keylife type.	option	-	seconds
	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
	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
	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.		

Parameter	Description	Type	Size	Default
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode
	Option	Description		
	<i>tunnel-mode</i>	Use tunnel mode encapsulation.		
	<i>transport-mode</i>	Use transport mode encapsulation.		
l2tp	Enable/disable L2TP over IPsec.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable L2TP over IPsec.		
	<i>disable</i>	Disable L2TP over IPsec.		
comments	Comment.	var-string	Maximum length: 255	
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
difffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
difffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified	
protocol	Quick mode protocol selector .	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	
src-addr-type	Local proxy ID type.	option	-	subnet

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
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 .	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
	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.		
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

Parameter	Description	Type	Size	Default
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 .	integer	Minimum value: 0 Maximum value: 65535	0

config vpn ipsec manualkey

Configure IPsec manual keys.

```
config vpn ipsec manualkey
  Description: Configure IPsec manual keys.
  edit <name>
    set interface {string}
    set remote-gw {ipv4-address}
    set local-gw {ipv4-address-any}
    set authentication [null|md5|...]
    set encryption [null|des|...]
    set authkey {user}
    set enckey {user}
    set localspi {user}
    set remotesspi {user}
    set npu-offload [enable|disable]
  next
end
```

config vpn ipsec manualkey

Parameter	Description	Type	Size	Default
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15	
remote-gw	Peer gateway.	ipv4-address	Not Specified	0.0.0.0
local-gw	Local gateway.	ipv4-address-any	Not Specified	0.0.0.0
authentication	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>null</i>	Null.		
	<i>md5</i>	MD5.		
	<i>sha1</i>	SHA1.		
	<i>sha256</i>	SHA256.		
	<i>sha384</i>	SHA384.		
	<i>sha512</i>	SHA512.		
encryption	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null
	Option	Description		
	<i>null</i>	Null.		
	<i>des</i>	DES.		
	<i>3des</i>	3DES.		
	<i>aes128</i>	AES128.		
	<i>aes192</i>	AES192.		
	<i>aes256</i>	AES256.		
	<i>aria128</i>	ARIA128.		
	<i>aria192</i>	ARIA192.		
	<i>aria256</i>	ARIA256.		
	<i>seed</i>	Seed.		
authkey	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified	
enckey	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified	
localspi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified	
remotespi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified	
npu-offload *	Enable/disable NPU offloading.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		

* This parameter may not exist in some models.

config vpn ipsec concentrator

Concentrator configuration.

```
config vpn ipsec concentrator
  Description: Concentrator configuration.
  edit <id>
    set name {string}
    set src-check [disable|enable]
    set member <name1>, <name2>, ...
  next
end
```

config vpn ipsec concentrator

Parameter	Description	Type	Size	Default
name	Concentrator name.	string	Maximum length: 35	
src-check	Enable to check source address of phase 2 selector. Disable to check only the destination selector.	option	-	disable
	Option	Description		
	<i>disable</i>	Ignore source selector when choosing tunnel.		
	<i>enable</i>	Use source selector to choose tunnel.		
member <name>	Names of up to 3 VPN tunnels to add to the concentrator. Member name.	string	Maximum length: 79	

config vpn ipsec phase1-interface

Configure VPN remote gateway.

```
config vpn ipsec phase1-interface
  Description: Configure VPN remote gateway.
  edit <name>
    set type [static|dynamic|...]
    set interface {string}
```

```

set ip-version [4|6]
set ike-version [1|2]
set local-gw {ipv4-address}
set local-gw6 {ipv6-address}
set remote-gw {ipv4-address}
set remote-gw6 {ipv6-address}
set remotegw-ddns {string}
set keylife {integer}
set certificate <name1>, <name2>, ...
set authmethod [psk|signature]
set authmethod-remote [psk|signature]
set mode [aggressive|main]
set peertype [any|one|...]
set peerid {string}
set default-gw {ipv4-address}
set default-gw-priority {integer}
set usrrgrp {string}
set peer {string}
set peergrp {string}
set monitor {string}
set monitor-hold-down-type [immediate|delay|...]
set monitor-hold-down-delay {integer}
set monitor-hold-down-weekday [everyday|sunday|...]
set monitor-hold-down-time {user}
set net-device [enable|disable]
set passive-mode [enable|disable]
set exchange-interface-ip [enable|disable]
set exchange-ip-addr4 {ipv4-address}
set exchange-ip-addr6 {ipv6-address}
set aggregate-member [enable|disable]
set aggregate-weight {integer}
set mode-cfg [disable|enable]
set assign-ip [disable|enable]
set assign-ip-from [range|usrrgrp|...]
set ipv4-start-ip {ipv4-address}
set ipv4-end-ip {ipv4-address}
set ipv4-netmask {ipv4-netmask}
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dns-mode [manual|auto]
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
set ipv4-split-include {string}
set split-include-service {string}
set ipv4-name {string}
set ipv6-start-ip {ipv6-address}
set ipv6-end-ip {ipv6-address}

```

```
set ipv6-prefix {integer}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set ipv6-split-include {string}
set ipv6-name {string}
set ip-delay-interval {integer}
set unity-support [disable|enable]
set domain {string}
set banner {var-string}
set include-local-lan [disable|enable]
set ipv4-split-exclude {string}
set ipv6-split-exclude {string}
set save-password [disable|enable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set backup-gateway <address1>, <address2>, ...
set proposal {option1}, {option2}, ...
set add-route [disable|enable]
set add-gw-route [enable|disable]
set psksecret {password-3}
set psksecret-remote {password-3}
set keepalive {integer}
set distance {integer}
set priority {integer}
set localid {string}
set localid-type [auto|fqdn|...]
set auto-negotiate [enable|disable]
set negotiate-timeout {integer}
set fragmentation [enable|disable]
set ip-fragmentation [pre-encapsulation|post-encapsulation]
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set forticlient-enforcement [enable|disable]
set comments {var-string}
set npu-offload [enable|disable]
set send-cert-chain [enable|disable]
set dhgrp {option1}, {option2}, ...
set suite-b [disable|suite-b-gcm-128|...]
set eap [enable|disable]
set eap-identity [use-id-payload|send-request]
set eap-exclude-peergrp {string}
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 authusrgroup {string}
set mesh-selector-type [disable|subnet|...]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ha-sync-esp-seqno [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 encapsulation [none|gre|...]
set encapsulation-address [ike|ipv4|...]
set encap-local-gw4 {ipv4-address}
set encap-local-gw6 {ipv6-address}
set encap-remote-gw4 {ipv4-address}
set encap-remote-gw6 {ipv6-address}
set vni {integer}
set nattraversal [enable|disable|...]
set esn [require|allow|...]
set fragmentation-mtu {integer}
set childless-ike [enable|disable]
set rekey [enable|disable]
set digital-signature-auth [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set rsa-signature-format [pkcs1|pss]
set enforce-unique-id [disable|keep-new|...]
set cert-id-validation [enable|disable]
set fec-egress [enable|disable]
set fec-send-timeout {integer}
set fec-base {integer}
set fec-codec {integer}
set fec-redundant {integer}
set fec-ingress [enable|disable]
set fec-receive-timeout {integer}
set network-overlay [disable|enable]
set network-id {integer}
set loopback-asymroute [enable|disable]
next
end

```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default
type	Remote gateway type.	option	-	static
	Option	Description		
	static	Remote VPN gateway has fixed IP address.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.		
	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.		
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35	
ip-version	IP version to use for VPN interface.	option	-	4
	Option	Description		
	4	Use IPv4 addressing for gateways.		
	6	Use IPv6 addressing for gateways.		
ike-version	IKE protocol version.	option	-	1
	Option	Description		
	1	Use IKEv1 protocol.		
	2	Use IKEv2 protocol.		
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
local-gw6	IPv6 address of the local gateway's external interface.	ipv6-address	Not Specified	::
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
remote-gw6	IPv6 address of the remote gateway's external interface.	ipv6-address	Not Specified	::
remotegw-ddns	Domain name of remote gateway (eg. name.DDNS.com).	string	Maximum length: 63	
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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>psk</i>	PSK authentication method.		
	<i>signature</i>	Signature authentication method.		
authmethod-remote	Authentication method (remote side).	option	-	
	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
	Option	Description		
	<i>aggressive</i>	Aggressive mode.		
	<i>main</i>	Main mode.		
peertype	Accept this peer type.	option	-	peer
	Option	Description		
	<i>any</i>	Accept any peer ID.		
	<i>one</i>	Accept this peer ID.		
	<i>dialup</i>	Accept peer ID in dialup group.		
	<i>peer</i>	Accept this peer certificate.		
	<i>peergrp</i>	Accept this peer certificate group.		
peerid	Accept this peer identity.	string	Maximum length: 255	
default-gw	IPv4 address of default route gateway to use for traffic exiting the interface.	ipv4-address	Not Specified	0.0.0.0
default-gw-priority	Priority for default gateway route. A higher priority number signifies a less preferred route.	integer	Minimum value: 0 Maximum value: 4294967295	0
usrgrp	User group name for dialup peers.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
peer	Accept this peer certificate.	string	Maximum length: 35	
peergrp	Accept this peer certificate group.	string	Maximum length: 35	
monitor	IPsec interface as backup for primary interface.	string	Maximum length: 35	
monitor-hold-down-type	Recovery time method when primary interface re-establishes.	option	-	immediate
	Option	Description		
	<i>immediate</i>	Fail back immediately after primary recovers.		
	<i>delay</i>	Number of seconds to delay fail back after primary recovers.		
	<i>time</i>	Specify a time at which to fail back after primary recovers.		
monitor-hold-down-delay	Time to wait in seconds before recovery once primary re-establishes.	integer	Minimum value: 0 Maximum value: 31536000	0
monitor-hold-down-weekday	Day of the week to recover once primary re-establishes.	option	-	sunday
	Option	Description		
	<i>everyday</i>	Every Day.		
	<i>sunday</i>	Sunday.		
	<i>monday</i>	Monday.		
	<i>tuesday</i>	Tuesday.		
	<i>wednesday</i>	Wednesday.		
	<i>thursday</i>	Thursday.		
	<i>friday</i>	Friday.		
	<i>saturday</i>	Saturday.		
monitor-hold-down-time	Time of day at which to fail back to primary after it re-establishes.	user	Not Specified	
net-device	Enable/disable kernel device creation.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Create a kernel device for every tunnel.		
	<i>disable</i>	Do not create a kernel device for tunnels.		
passive-mode	Enable/disable IPsec passive mode for static tunnels.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPsec passive mode.		
	<i>disable</i>	Disable IPsec passive mode.		
exchange-interface-ip	Enable/disable exchange of IPsec interface IP address.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable exchange of IPsec interface IP address.		
	<i>disable</i>	Disable exchange of IPsec interface IP address.		
exchange-ip-addr4	IPv4 address to exchange with peers.	ipv4-address	Not Specified	0.0.0.0
exchange-ip-addr6	IPv6 address to exchange with peers	ipv6-address	Not Specified	::
aggregate-member	Enable/disable use as an aggregate member.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use as an aggregate member.		
	<i>disable</i>	Disable use as an aggregate member.		
aggregate-weight	Link weight for aggregate.	integer	Minimum value: 1 Maximum value: 100	1
mode-cfg	Enable/disable configuration method.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Configuration Method.		
	<i>enable</i>	Enable Configuration Method.		

Parameter	Description	Type	Size	Default
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable
	Option	Description		
	<i>disable</i>	Do not assign an IP address to the IPsec interface.		
	<i>enable</i>	Assign an IP address to the IPsec interface.		
assign-ip-from	Method by which the IP address will be assigned.	option	-	range
	Option	Description		
	<i>range</i>	Assign IP address from locally defined range.		
	<i>usrgrp</i>	Assign IP address via user group.		
	<i>dhcp</i>	Assign IP address via DHCP.		
	<i>name</i>	Assign IP address from firewall address or group.		
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::
dns-mode	DNS server mode.	option	-	manual
	Option	Description		
	<i>manual</i>	Manually configure DNS servers.		
	<i>auto</i>	Use default DNS servers.		
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
split-include-service	Split-include services.	string	Maximum length: 79	
ipv4-name	IPv4 address name.	string	Maximum length: 79	
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79	
ipv6-name	IPv6 address name.	string	Maximum length: 79	
ip-delay-interval	IP address reuse delay interval in seconds .	integer	Minimum value: 0 Maximum value: 28800	0
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable
Option	Description			
disable	Disable Cisco Unity Configuration Method Extensions.			
enable	Enable Cisco Unity Configuration Method Extensions.			
domain	Instruct unity clients about the default DNS domain.	string	Maximum length: 63	
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024	
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable
Option	Description			
disable	Disable local LAN access on Unity clients.			
enable	Enable local LAN access on Unity clients.			

Parameter	Description	Type	Size	Default	
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79		
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79		
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable	
Option		Description			
		<code>disable</code>	Disable saving XAuth username and password on VPN clients.		
		<code>enable</code>	Enable saving XAuth username and password on VPN clients.		
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable	
Option		Description			
		<code>disable</code>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.		
		<code>enable</code>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.		
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable	
Option		Description			
		<code>disable</code>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.		
		<code>enable</code>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.		
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79		
proposal	Phase1 proposal.	option	-		
Option		Description			
		<code>des-md5</code>	des-md5		
		<code>des-sha1</code>	des-sha1		
		<code>des-sha256</code>	des-sha256		

Parameter	Description	Type	Size	Default
	Option	Description		
	<code>des-sha384</code>	des-sha384		
	<code>des-sha512</code>	des-sha512		
	<code>3des-md5</code>	3des-md5		
	<code>3des-sha1</code>	3des-sha1		
	<code>3des-sha256</code>	3des-sha256		
	<code>3des-sha384</code>	3des-sha384		
	<code>3des-sha512</code>	3des-sha512		
	<code>aes128-md5</code>	aes128-md5		
	<code>aes128-sha1</code>	aes128-sha1		
	<code>aes128-sha256</code>	aes128-sha256		
	<code>aes128-sha384</code>	aes128-sha384		
	<code>aes128-sha512</code>	aes128-sha512		
	<code>aes128gcm-prfsha1</code>	aes128gcm-prfsha1		
	<code>aes128gcm-prfsha256</code>	aes128gcm-prfsha256		
	<code>aes128gcm-prfsha384</code>	aes128gcm-prfsha384		
	<code>aes128gcm-prfsha512</code>	aes128gcm-prfsha512		
	<code>aes192-md5</code>	aes192-md5		
	<code>aes192-sha1</code>	aes192-sha1		
	<code>aes192-sha256</code>	aes192-sha256		
	<code>aes192-sha384</code>	aes192-sha384		
	<code>aes192-sha512</code>	aes192-sha512		
	<code>aes256-md5</code>	aes256-md5		
	<code>aes256-sha1</code>	aes256-sha1		
	<code>aes256-sha256</code>	aes256-sha256		
	<code>aes256-sha384</code>	aes256-sha384		
	<code>aes256-sha512</code>	aes256-sha512		
	<code>aes256gcm-prfsha1</code>	aes256gcm-prfsha1		
	<code>aes256gcm-prfsha256</code>	aes256gcm-prfsha256		
	<code>aes256gcm-prfsha384</code>	aes256gcm-prfsha384		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1		
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256		
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384		
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		
	<i>aria192-sha384</i>	aria192-sha384		
	<i>aria192-sha512</i>	aria192-sha512		
	<i>aria256-md5</i>	aria256-md5		
	<i>aria256-sha1</i>	aria256-sha1		
	<i>aria256-sha256</i>	aria256-sha256		
	<i>aria256-sha384</i>	aria256-sha384		
	<i>aria256-sha512</i>	aria256-sha512		
	<i>seed-md5</i>	seed-md5		
	<i>seed-sha1</i>	seed-sha1		
	<i>seed-sha256</i>	seed-sha256		
	<i>seed-sha384</i>	seed-sha384		
	<i>seed-sha512</i>	seed-sha512		
add-route	Enable/disable control addition of a route option to peer destination selector.	-	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Do not add a route to destination of peer selector.		
	<i>enable</i>	Add route to destination of peer selector.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable
	Option	Description		
	<i>enable</i>	Automatically add a route to the remote gateway.		
	<i>disable</i>	Do not automatically add a route to the remote gateway.		
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255	15
priority	Priority for routes added by IKE .	integer	Minimum value: 0 Maximum value: 4294967295	0
localid	Local ID.	string	Maximum length: 63	
localid-type	Local ID type.	option	-	auto
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>keyid</i>	Use key-id string.		
	<i>address</i>	Use local IP address.		
	<i>asn1dn</i>	Use ASN.1 distinguished name.		
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.		
	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.		
negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300	30
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.		
	<i>disable</i>	Disable intra-IKE fragmentation support.		
ip-fragmentation	Determine whether IP packets are fragmented before or after IPsec encapsulation.	option	-	post-encapsulation
	Option	Description		
	<i>pre-encapsulation</i>	Fragment before IPsec encapsulation.		
	<i>post-encapsulation</i>	Fragment after IPsec encapsulation (RFC compliant).		
dpd	Dead Peer Detection mode.	option	-	on-demand
	Option	Description		
	<i>disable</i>	Disable Dead Peer Detection.		
	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.		
	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.		

Parameter	Description	Type	Size	Default
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3
dpd-retryinterval	DPD retry interval.	user	Not Specified	
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-	disable
Option		Description		
		<i>enable</i> Enable FortiClient enforcement.		
		<i>disable</i> Disable FortiClient enforcement.		
comments	Comment.	var-string	Maximum length: 255	
npu-offload *	Enable/disable offloading NPU.	option	-	enable
Option		Description		
		<i>enable</i> Enable NPU offloading.		
		<i>disable</i> Disable NPU offloading.		
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable
Option		Description		
		<i>enable</i> Enable sending certificate chain.		
		<i>disable</i> Disable sending certificate chain.		
dhgrp	DH group.	option	-	14
Option		Description		
		1 DH Group 1.		
		2 DH Group 2.		
		5 DH Group 5.		
		14 DH Group 14.		
		15 DH Group 15.		
		16 DH Group 16.		
		17 DH Group 17.		
		18 DH Group 18.		

Parameter	Description	Type	Size	Default
	Option	Description		
	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.		
suite-b	Use Suite-B.	option	-	disable
	Option	Description		
	disable	Do not use UI suite.		
	suite-b-gcm-128	Use Suite-B-GCM-128.		
	suite-b-gcm-256	Use Suite-B-GCM-256.		
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable
	Option	Description		
	enable	Enable IKEv2 EAP authentication.		
	disable	Disable IKEv2 EAP authentication.		
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload
	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	
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable

Parameter	Description	Type	Size	Default
	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.		
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.		
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.		
	<i>static-fortigate</i>	Site to Site - FortiGate.		
	<i>dialup-fortigate</i>	Dial Up - FortiGate.		
	<i>static-cisco</i>	Site to Site - Cisco.		
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.		
	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).		
	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.		
	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.		

Parameter	Description	Type	Size	Default												
xauthtype	XAuth type.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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.															
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 IDi group authentication. (ASCII string or hexadecimal indicated by a leading 0x.)	password-3	Not Specified													
authusgrp	Authentication user group.	string	Maximum length: 35													
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable.</td></tr> <tr> <td><i>subnet</i></td><td>Enable addition of matching subnet selector.</td></tr> <tr> <td><i>host</i></td><td>Enable addition of host to host selector.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable.	<i>subnet</i>	Enable addition of matching subnet selector.	<i>host</i>	Enable addition of host to host selector.							
Option	Description															
<i>disable</i>	Disable.															
<i>subnet</i>	Enable addition of matching subnet selector.															
<i>host</i>	Enable addition of host to host selector.															

Parameter	Description	Type	Size	Default
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable
	Option	Description		
	enable	Enable IPsec tunnel idle timeout.		
	disable	Disable IPsec tunnel idle timeout.		
idle-timeoutinterval	IPsec tunnel idle timeout in minutes .	integer	Minimum value: 5 Maximum value: 43200	15
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable
	Option	Description		
	enable	Enable HA syncing of ESP sequence numbers.		
	disable	Disable HA syncing of ESP sequence numbers.		
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable
	Option	Description		
	enable	Enable sending auto-discovery short-cut messages.		
	disable	Disable sending auto-discovery short-cut messages.		
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable
	Option	Description		
	enable	Enable receiving auto-discovery short-cut messages.		
	disable	Disable receiving auto-discovery short-cut messages.		
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable
	Option	Description		
	enable	Enable forwarding auto-discovery short-cut messages.		
	disable	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

Parameter	Description	Type	Size	Default
	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
	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.		
encapsulation	Enable/disable GRE/VXLAN encapsulation.	option	-	none
	Option	Description		
	<i>none</i>	No additional encapsulation.		
	<i>gre</i>	GRE encapsulation.		
	<i>vxlan</i>	VXLAN encapsulation.		
encapsulation-address	Source for GRE/VXLAN tunnel address.	option	-	ike
	Option	Description		
	<i>ike</i>	Use IKE/IPsec gateway addresses.		
	<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.		
	<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.		
encap-local-gw4	Local IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0
encap-local-gw6	Local IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::
encap-remote-gw4	Remote IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0
encap-remote-gw6	Remote IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default								
vni	VNI of VXLAN tunnel.	integer	Minimum value: 1 Maximum value: 16777215	0								
natTraversal	Enable/disable NAT traversal.	option	-	enable								
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable IPsec NAT traversal.</td></tr> <tr> <td><i>disable</i></td><td>Disable IPsec NAT traversal.</td></tr> <tr> <td><i>forced</i></td><td>Force IPsec NAT traversal on.</td></tr> </tbody> </table>			Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.
Option	Description											
<i>enable</i>	Enable IPsec NAT traversal.											
<i>disable</i>	Disable IPsec NAT traversal.											
<i>forced</i>	Force IPsec NAT traversal on.											
esn *	Extended sequence number (ESN) negotiation.	option	-	disable								
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>require</i></td><td>Require extended sequence number.</td></tr> <tr> <td><i>allow</i></td><td>Allow extended sequence number.</td></tr> <tr> <td><i>disable</i></td><td>Disable extended sequence number.</td></tr> </tbody> </table>			Option	Description	<i>require</i>	Require extended sequence number.	<i>allow</i>	Allow extended sequence number.	<i>disable</i>	Disable extended sequence number.
Option	Description											
<i>require</i>	Require extended sequence number.											
<i>allow</i>	Allow extended sequence number.											
<i>disable</i>	Disable extended sequence number.											
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000	1200								
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable								
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr> <tr> <td><i>disable</i></td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr> </tbody> </table>			Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).		
Option	Description											
<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).											
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).											
rekey	Enable/disable phase1 rekey.	option	-	enable								
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable phase1 rekey.</td></tr> <tr> <td><i>disable</i></td><td>Disable phase1 rekey.</td></tr> </tbody> </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								

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>sha1</i>	SHA1.		
	<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
	Option	Description		
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.		
	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).		
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable
	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
	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.		
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.		
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 1000	8
fec-base	Number of base Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100	20
fec-codec	ipsec fec encoding/decoding algorithm (0: reed-solomon, 1: xor).	integer	Minimum value: 0 Maximum value: 1	0
fec-redundant	Number of redundant Forward Error Correction packets (0 - 100, when fec-codec is reed-solomon or 1 when fec-codec is xor .	integer	Minimum value: 0 Maximum value: 100	1
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.		
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 10000	5000
network-overlay	Enable/disable network overlays.	option	-	disable
	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

Parameter	Description	Type	Size	Default
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable
Parameter	Description	Type	Size	Default
enable	Allow ingress/egress IKE traffic to be routed over different interfaces.			
disable	Ingress/egress IKE traffic must be routed over the same interface.			

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

config ipv6-exclude-range

Parameter	Description	Type	Size	Default
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::

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 dhcp-ipsec [enable|disable]
    set proposal {option1}, {option2}, ...
    set pfs [enable|disable]
    set ipv4-df [enable|disable]
    set dhgrp {option1}, {option2}, ...
    set replay [enable|disable]
    set keepalive [enable|disable]
    set auto-negotiate [enable|disable]
    set add-route [phase1|enable|...]
    set auto-discovery-sender [phase1|enable|...]
    set auto-discovery-forwarder [phase1|enable|...]
    set keylifeseconds {integer}
```

```

set keylife{kbs {integer}
set keylife-type [seconds|kbs|...]
set single-source [enable|disable]
set route-overlap [use-old|use-new|...]
set encapsulation [tunnel-mode|transport-mode]
set l2tp [enable|disable]
set comments {var-string}
set initiator-ts-narrow [enable|disable]
set diffserv [enable|disable]
set diffservcode {user}
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
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15	
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable
Option		Description		
		<i>enable</i> Enable setting.		
		<i>disable</i> Disable setting.		
proposal	Phase2 proposal.	option	-	

Parameter	Description	Type	Size	Default
Option	Description			
<i>null-md5</i>	null-md5			
<i>null-sha1</i>	null-sha1			
<i>null-sha256</i>	null-sha256			
<i>null-sha384</i>	null-sha384			
<i>null-sha512</i>	null-sha512			
<i>des-null</i>	des-null			
<i>des-md5</i>	des-md5			
<i>des-sha1</i>	des-sha1			
<i>des-sha256</i>	des-sha256			
<i>des-sha384</i>	des-sha384			
<i>des-sha512</i>	des-sha512			
<i>3des-null</i>	3des-null			
<i>3des-md5</i>	3des-md5			
<i>3des-sha1</i>	3des-sha1			
<i>3des-sha256</i>	3des-sha256			
<i>3des-sha384</i>	3des-sha384			
<i>3des-sha512</i>	3des-sha512			
<i>aes128-null</i>	aes128-null			
<i>aes128-md5</i>	aes128-md5			
<i>aes128-sha1</i>	aes128-sha1			
<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			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-null</i>	aria192-null		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		
	<i>aria192-sha384</i>	aria192-sha384		
	<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		

Parameter	Description	Type	Size	Default
	Option	Description		
	<code>seed-sha1</code>	seed-sha1		
	<code>seed-sha256</code>	seed-sha256		
	<code>seed-sha384</code>	seed-sha384		
	<code>seed-sha512</code>	seed-sha512		
pfs	Enable/disable PFS feature.	option	-	enable
	Option	Description		
	<code>enable</code>	Enable setting.		
	<code>disable</code>	Disable setting.		
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-	disable
	Option	Description		
	<code>enable</code>	Set IPv4 DF.		
	<code>disable</code>	Reset IPv4 DF.		
dhgrp	Phase2 DH group.	option	-	14
	Option	Description		
	<code>1</code>	DH Group 1.		
	<code>2</code>	DH Group 2.		
	<code>5</code>	DH Group 5.		
	<code>14</code>	DH Group 14.		
	<code>15</code>	DH Group 15.		
	<code>16</code>	DH Group 16.		
	<code>17</code>	DH Group 17.		
	<code>18</code>	DH Group 18.		
	<code>19</code>	DH Group 19.		
	<code>20</code>	DH Group 20.		
	<code>21</code>	DH Group 21.		
	<code>27</code>	DH Group 27.		
	<code>28</code>	DH Group 28.		

Parameter	Description	Type	Size	Default
	Option	Description		
	29	DH Group 29.		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		
replay	Enable/disable replay detection.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
keepalive	Enable/disable keep alive.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
add-route	Enable/disable automatic route addition.	option	-	phase1
	Option	Description		
	phase1	Add route according to phase1 add-route setting.		
	enable	Add route for remote proxy ID.		
	disable	Do not add route for remote proxy ID.		
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1
	Option	Description		
	phase1	Send short-cut messages according to the phase1 auto-discovery-sender setting.		
	enable	Enable sending auto-discovery short-cut messages.		
	disable	Disable sending auto-discovery short-cut messages.		

Parameter	Description	Type	Size	Default
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1
	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.		
keylifesecs	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800	43200
keylifekbs	Phase2 key life in number of bytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295	5120
keylife-type	Keylife type.	option	-	seconds
	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
	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
	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.		
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tunnel-mode</i>	Use tunnel mode encapsulation.		
	<i>transport-mode</i>	Use transport mode encapsulation.		
l2tp	Enable/disable L2TP over IPsec.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable L2TP over IPsec.		
	<i>disable</i>	Disable L2TP over IPsec.		
comments	Comment.	var-string	Maximum length: 255	
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified	
protocol	Quick mode protocol selector .	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	
src-addr-type	Local proxy ID type.	option	-	subnet

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
	<i>subnet6</i>	IPv6 subnet.		
	<i>range6</i>	IPv6 range.		
	<i>ip6</i>	IPv6 IP.		
	<i>name6</i>	IPv6 firewall address or group name.		
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 .	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
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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 .	integer	Minimum value: 0 Maximum value: 65535	0

config vpn ipsec manualkey-interface

Configure IPsec manual keys.

```
config vpn ipsec manualkey-interface
  Description: Configure IPsec manual keys.
  edit <name>
    set interface {string}
    set ip-version [4|6]
    set addr-type [4|6]
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set auth-alg [null|md5|...]
    set enc-alg [null|des|...]
    set auth-key {user}
    set enc-key {user}
    set local-spi {user}
    set remote-spi {user}
    set npu-offload [enable|disable]
  next
end
```

config vpn ipsec manualkey-interface

Parameter	Description	Type	Size	Default
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15	
ip-version	IP version to use for VPN interface.	option	-	4
Option	Description			
4	Use IPv4 addressing for gateways.			
6	Use IPv6 addressing for gateways.			
addr-type	IP version to use for IP packets.	option	-	4
Option	Description			
4	Use IPv4 addressing for IP packets.			
6	Use IPv6 addressing for IP packets.			
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
remote-gw6	Remote IPv6 address of VPN gateway.	ipv6-address	Not Specified	::
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address-any	Not Specified	0.0.0.0
local-gw6	Local IPv6 address of VPN gateway.	ipv6-address	Not Specified	::
auth-alg	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null
Option	Description			
<i>null</i>	null			
<i>md5</i>	md5			
<i>sha1</i>	sha1			
<i>sha256</i>	sha256			
<i>sha384</i>	sha384			
<i>sha512</i>	sha512			
enc-alg	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>null</i>	null		
	<i>des</i>	des		
	<i>3des</i>	3des		
	<i>aes128</i>	aes128		
	<i>aes192</i>	aes192		
	<i>aes256</i>	aes256		
	<i>aria128</i>	aria128		
	<i>aria192</i>	aria192		
	<i>aria256</i>	aria256		
	<i>seed</i>	seed		
auth-key	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user		Not Specified
enc-key	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user		Not Specified
local-spi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user		Not Specified
remote-spi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user		Not Specified
npu-offload *	Enable/disable offloading IPsec VPN manual key sessions to NPUs.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		

* This parameter may not exist in some models.

config vpn ipsec forticlient

Configure FortiClient policy realm.

```
config vpn ipsec forticlient
  Description: Configure FortiClient policy realm.
  edit <realm>
    set usergroupname {string}
    set phase2name {string}
```

```
        set status [enable|disable]
    next
end
```

config vpn ipsec forticlient

Parameter	Description	Type	Size	Default
usergroupname	User group name for FortiClient users.	string	Maximum length: 35	
phase2name	Phase 2 tunnel name that you defined in the FortiClient dialup configuration.	string	Maximum length: 35	
status	Enable/disable this FortiClient configuration.	option	-	enable
Option		Description		
		enable	Enable setting.	
		disable	Disable setting.	

config vpn ipsec stats crypto

IPsec crypto statistics.

```
config vpn ipsec stats crypto
    Description: IPsec crypto statistics.
end
```

config vpn ipsec stats tunnel

IPsec tunnel statistics.

```
config vpn ipsec stats tunnel
    Description: IPsec tunnel statistics.
end
```

config vpn ipsec tunnel details

List all IPsec tunnels in details.

```
config vpn ipsec tunnel details
    Description: List all IPsec tunnels in details.
end
```

config vpn ipsec tunnel summary

List all IPsec tunnels in summary.

```
config vpn ipsec tunnel summary
```

```
Description: List all IPsec tunnels in summary.  
end
```

config vpn ipsec tunnel name

List IPsec tunnel by name.

```
config vpn ipsec tunnel name  
    Description: List IPsec tunnel by name.  
end
```

config vpn pptp

Configure PPTP.

```
config vpn pptp  
    Description: Configure PPTP.  
    set status [enable|disable]  
    set ip-mode [range|usrgrp]  
    set eip {ipv4-address}  
    set sip {ipv4-address}  
    set local-ip {ipv4-address}  
    set usrgrp {string}  
end
```

config vpn pptp

Parameter	Description		Type	Size	Default
status	Enable/disable FortiGate as a PPTP gateway.		option	-	disable
	Option		Description		
	<i>enable</i>		Enable setting.		
	<i>disable</i>		Disable setting.		
ip-mode	IP assignment mode for PPTP client.		option	-	range
	Option		Description		
	<i>range</i>		PPTP client IP from manual config (range from sip to eip).		
	<i>usrgrp</i>		PPTP client IP from user-group defined server.		
eip	End IP.		ipv4-address	Not Specified	0.0.0.0
sip	Start IP.		ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
local-ip	Local IP to be used for peer's remote IP.	ipv4-address	Not Specified	0.0.0.0
usrgrp	User group.	string	Maximum length: 35	

config vpn l2tp

Configure L2TP.

```
config vpn l2tp
    Description: Configure L2TP.
    set status [enable|disable]
    set eip {ipv4-address}
    set sip {ipv4-address}
    set usrgrp {string}
    set enforce-ipsec [enable|disable]
    set lcp-echo-interval {integer}
    set lcp-max-echo-fails {integer}
    set hello-interval {integer}
    set compress [enable|disable]
end
```

config vpn l2tp

Parameter	Description	Type	Size	Default
status	Enable/disable FortiGate as a L2TP gateway.	option	-	disable
Parameter	Description	Type	Size	Default
eip	End IP.	ipv4-address	Not Specified	0.0.0.0
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0
usrgrp	User group.	string	Maximum length: 35	
enforce-ipsec	Enable/disable IPsec enforcement.	option	-	disable
Parameter	Description	Type	Size	Default

Parameter	Description	Type	Size	Default
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5
lcp-max-echo-fails	Maximum number of missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3
hello-interval	L2TP hello message interval in seconds .	integer	Minimum value: 0 Maximum value: 3600	60
compress	Enable/disable data compression.	option	-	disable
Option	Description			
enable	Enable compress			
disable	Disable compress			

config vpn ovpn

Configure Overlay Controller VPN settings.

```
config vpn ovpn
    Description: Configure Overlay Controller VPN settings.
    set status [enable|disable]
    set role [spoke|primary-hub|...]
    set multipath [enable|disable]
    set sdwan [enable|disable]
    set sdwan-zone {string}
    set wan-interface <name1>, <name2>, ...
    set nat [enable|disable]
    set ip-allocation-block {ipv4-classnet-any}
    config overlays
        Description: Network overlays to register with Overlay Controller VPN service.
        edit <overlay-name>
            set inter-overlay [allow|deny]
            config subnets
                Description: Internal subnets to register with OCVPN service.
                edit <id>
                    set type [subnet|interface]
                    set subnet {ipv4-classnet-any}
                    set interface {string}
                next
            end
        next
    end
```

```

config forticlient-access
Description: Configure FortiClient settings.
set status {enable|disable}
set psksecret {password-3}
config auth-groups
Description: FortiClient user authentication groups.
edit <name>
    set auth-group {string}
    set overlays <overlay-name1>, <overlay-name2>, ...
next
end
end
set auto-discovery [enable|disable]
set auto-discovery-shortcut-mode [independent|dependent]
set poll-interval {integer}
set eap [enable|disable]
    set eap-users {string}
end

```

config vpn ovpn

Parameter	Description	Type	Size	Default
status	Enable/disable Overlay Controller cloud assisted VPN.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Overlay Controller VPN.		
	<i>disable</i>	Disable Overlay Controller VPN.		
role	Set device role.	option	-	spoke
	Option	Description		
	<i>spoke</i>	Register device as static spoke.		
	<i>primary-hub</i>	Register device as primary hub.		
	<i>secondary-hub</i>	Register device as secondary hub.		
multipath	Enable/disable multipath redundancy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multipath redundancy.		
	<i>disable</i>	Disable multipath redundancy.		
sdwan	Enable/disable adding OVPN tunnels to SD-WAN.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable adding OVPN tunnels to SD-WAN.		
	<i>disable</i>	Disable adding OVPN tunnels to SD-WAN.		
sdwan-zone	Set SD-WAN zone.	string	Maximum length: 35	virtual-wan-link
wan-interface <name>	FortiGate WAN interfaces to use with OVPN. Interface name.	string	Maximum length: 79	
nat	Enable/disable NAT support.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable NAT support.		
	<i>disable</i>	Disable NAT support.		
ip-allocation-block	Class B subnet reserved for private IP address assignment.	ipv4-classnet-any	Not Specified	10.254.0.0 255.255.0.0
auto-discovery	Enable/disable auto-discovery shortcuts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ADVVPN auto-discovery shortcuts.		
	<i>disable</i>	Disable ADVVPN auto-discovery shortcuts.		
auto-discovery-shortcut-mode	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent
	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.		
poll-interval	Overlay Controller VPN polling interval.	integer	Minimum value: 30 Maximum value: 120	30
eap	Enable/disable EAP client authentication.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable EAP client authentication.		
	<i>disable</i>	Disable EAP client authentication.		
eap-users	EAP authentication user group.	string	Maximum length: 35	

config overlays

Parameter	Description	Type	Size	Default
inter-overlay	Allow or deny traffic from other overlays.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow traffic from other overlays.		
	<i>deny</i>	Deny traffic from other overlays.		

config subnets

Parameter	Description	Type	Size	Default
type	Subnet type.	option	-	subnet
	Option	Description		
	<i>subnet</i>	Configure participating subnet IP and mask.		
	<i>interface</i>	Configure participating LAN interface.		
subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
interface	LAN interface.	string	Maximum length: 15	

config forticlient-access

Parameter	Description	Type	Size	Default
status	Enable/disable FortiClient to access OVPN networks.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiClient access to OVPN overlays.		
	<i>disable</i>	Disable FortiClient access to OVPN overlays.		

Parameter	Description	Type	Size	Default
psksecret	Pre-shared secret for FortiClient PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	

config auth-groups

Parameter	Description	Type	Size	Default
auth-group	Authentication user group for FortiClient access.	string	Maximum length: 35	
overlays <overlay-name>	OCVPN overlays to allow access to. Overlay name.	string	Maximum length: 79	

config vpn ike gateway

List gateways.

```
config vpn ike gateway
  Description: List gateways.
  set <name> {string}
end
```

config vpn ike gateway

Parameter	Description	Type	Size	Default
<name>	Name of IKE gateway to list.	string	Maximum length: -1	

config vpn status l2tp

Display L2TP status.

```
config vpn status l2tp
  Description: Display L2TP status.
end
```

config vpn status pptp

Display PPTP status.

```
config vpn status pptp
  Description: Display PPTP status.
end
```

config vpn status ssl list

List current connections.

```
config vpn status ssl list
    Description: List current connections.
end
```

config vpn status ssl hw-acceleration-status

SSL hardware acceleration status.

```
config vpn status ssl hw-acceleration-status
    Description: SSL hardware acceleration status.
end
```

waf

This section includes syntax for the following commands:

- [config waf profile on page 1478](#)
- [config waf signature on page 1478](#)
- [config waf sub-class on page 1477](#)
- [config waf main-class on page 1477](#)

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	

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	

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	

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
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
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
    end
next
end
set comment {var-string}
next
end

```

config waf profile

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
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	-	enable
	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 custom-signature

Parameter	Description	Type	Size	Default
status	Status.	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.		

Parameter	Description	Type	Size	Default		
	Option	Description				
	<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			
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.				

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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
	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.		

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 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
	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
	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.		

Parameter	Description	Type	Size	Default								
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024								
action	Action.	option	-	allow								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>allow</i></td><td>Allow.</td></tr> <tr> <td><i>block</i></td><td>Block.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 url-param-length

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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	Maximum length of URL parameter 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 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.		
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 method

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 method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable

Parameter	Description	Type	Size	Default
	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.		
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 hostname

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	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.		
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

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-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
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-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
	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
	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.		

Parameter	Description	Type	Size	Default								
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								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>allow</i></td><td>Allow.</td></tr> <tr> <td><i>block</i></td><td>Block.</td></tr> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 exception

Parameter	Description	Type	Size	Default						
pattern	URL pattern.	string	Maximum length: 511							
regex	Enable/disable regular expression based pattern match.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>	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						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
content-length	HTTP content length in request.	option	-	disable
	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
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
line-length	HTTP line length in request.	option	-	disable
	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

Parameter	Description	Type	Size	Default
	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
	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

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

config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
action	Action.	option	-	allow
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium

config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium
default-allowed-methods	Methods.	option	-	

config method-policy

Parameter	Description	Type	Size	Default
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.		
address	Host address.	string	Maximum length: 79	
allowed-methods	Allowed Methods.	option	-	

Parameter	Description	Type	Size	Default
	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.		
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	

config url-access

Parameter	Description	Type	Size	Default
address	Host address.	string	Maximum length: 79	
action	Action.	option	-	permit
Option	Description			
<i>bypass</i>	Allow the HTTP request, also bypass further WAF scanning.			
<i>permit</i>	Allow the HTTP request, and continue further WAF scanning.			
<i>block</i>	Block HTTP request.			
log	Enable/disable logging.	option	-	disable
Option	Description			
<i>enable</i>	Enable setting.			
<i>disable</i>	Disable setting.			
severity	Severity.	option	-	medium
Option	Description			
<i>high</i>	High severity.			
<i>medium</i>	Medium severity.			
<i>low</i>	Low severity.			

config access-pattern

Parameter	Description	Type	Size	Default
srcaddr	Source address.	string	Maximum length: 79	
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
negate	Enable/disable match negation.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

web-proxy

This section includes syntax for the following commands:

- [config web-proxy forward-server on page 1514](#)
- [config web-proxy explicit on page 1509](#)
- [config web-proxy url-match on page 1519](#)
- [config web-proxy profile on page 1503](#)
- [config web-proxy debug-url on page 1517](#)
- [config web-proxy global on page 1507](#)
- [config web-proxy wisp on page 1518](#)
- [config web-proxy forward-server-group on page 1516](#)

config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
    Description: Configure web proxy profiles.
    edit <name>
        set header-client-ip [pass|add|...]
        set header-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
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
Option				
<i>pass</i>				
Forward the same HTTP header.				
<i>add</i>				
Add the HTTP header.				
<i>remove</i>				
Remove the HTTP header.				
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
Option				
<i>pass</i>				
Forward the same HTTP header.				
<i>add</i>				
Add the HTTP header.				
<i>remove</i>				
Remove the HTTP header.				
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-	pass
Option				
<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
Option				
<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

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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-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								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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-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								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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.											
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>enable</i></td> <td>Enable stripping of unsupported encoding from the request header.</td> </tr> <tr> <td><i>disable</i></td> <td>Disable stripping of unsupported encoding from the request header.</td> </tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable stripping of unsupported encoding from the request header.	<i>disable</i>	Disable stripping of unsupported encoding from the request header.					
Option	Description											
<i>enable</i>	Enable stripping of unsupported encoding from the request header.											
<i>disable</i>	Disable stripping of unsupported encoding from the request header.											

Parameter	Description	Type	Size	Default
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
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	Action when the HTTP header is forwarded.	option	-	add-to-request
	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.		
content	HTTP header content.	string	Maximum length: 255	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of base64 encoding of HTTP content.		
	<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

Parameter	Description	Type	Size	Default
	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.		
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-	https http
	Option	Description		
	<i>https</i>	Perform add-option action on HTTPS.		
	<i>http</i>	Perform add-option action on HTTP.		

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 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 max-waf-body-cache-length {integer}
  set webproxy-profile {string}
  set learn-client-ip [enable|disable]
  set learn-client-ip-from-header {option1}, {option2}, ...
  set learn-client-ip-srcaddr <name1>, <name2>, ...
  set learn-client-ip-srcaddr6 <name1>, <name2>, ...
  set src-affinity-exempt-addr {ipv4-address-any}
  set src-affinity-exempt-addr6 {ipv6-address}
end
```

config web-proxy global

Parameter	Description	Type	Size	Default
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	Fortinet_Factory

Parameter	Description	Type	Size	Default
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	Fortinet_CA_SSL
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.		
proxy-fqdn	Fully Qualified Domain Name to connect to the explicit web proxy.	string	Maximum length: 255	default.fqdn
max-request-length	Maximum length of HTTP request line .	integer	Minimum value: 2 Maximum value: 64	8
max-message-length	Maximum length of HTTP message, not including body .	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
	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
	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 .	integer	Minimum value: 6 Maximum value: 60	30

Parameter	Description	Type	Size	Default
max-waf-body-cache-length	Maximum length of HTTP messages processed by Web Application Firewall .	integer	Minimum value: 10 Maximum value: 1024	32
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	Enable/disable learning the client's IP address from headers.	option	-	disable
Option		Description		
		<i>enable</i> Enable learning the client's IP address from headers.		
		<i>disable</i> Disable learning the client's IP address from headers.		
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-	
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	

config web-proxy explicit

Configure explicit Web proxy settings.

```
config web-proxy explicit
  Description: Configure explicit Web proxy settings.
  set status [enable|disable]
```

```

set ftp-over-http [enable|disable]
set socks [enable|disable]
set http-incoming-port {user}
set https-incoming-port {user}
set ftp-incoming-port {user}
set socks-incoming-port {user}
set incoming-ip {ipv4-address-any}
set outgoing-ip {ipv4-address-any}
set ipv6-status [enable|disable]
set incoming-ip6 {ipv6-address}
set outgoing-ip6 {ipv6-address}
set strict-guest [enable|disable]
set pref-dns-result [ipv4|ipv6]
set unknown-http-version [reject|best-effort]
set realm {string}
set sec-default-action [accept|deny]
set https-replacement-message [enable|disable]
set message-upon-server-error [enable|disable]
set pac-file-server-status [enable|disable]
set pac-file-url {user}
set pac-file-server-port {user}
set pac-file-name {string}
set pac-file-data {user}
config pac-policy
    Description: PAC policies.
    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
set ssl-algorithm [high|medium|...]
set trace-auth-no-rsp [enable|disable]
end

```

config web-proxy explicit

Parameter	Description	Type	Size	Default
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.		
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable

Parameter	Description	Type	Size	Default
	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
	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 .	user	Not Specified	
https-incoming-port	Accept incoming HTTPS requests on one or more ports .	user	Not Specified	
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports .	user	Not Specified	
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports .	user	Not Specified	
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
outgoing-ip	Outgoing HTTP requests will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified	
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable allowing an IPv6 web proxy destination.		
	<i>disable</i>	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	::
outgoing-ip6	Outgoing HTTP requests will leave this IPv6. Multiple interfaces can be specified. Interfaces must have these IPv6 addresses.	ipv6-address	Not Specified	

Parameter	Description	Type	Size	Default
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable strict guest user checking.		
	<i>disable</i>	Disable strict guest user checking.		
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server .	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	Prefer the IPv4 DNS server.		
	<i>ipv6</i>	Prefer the IPv6 DNS server.		
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject
	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.		
https-replacement-message	Enable/disable sending the client a replacement message for HTTPS requests.	option	-	enable
	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 displaying a replacement message when a server error is detected.	option	-	enable
	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.		
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 .	user	Not Specified	
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
	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.		
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging timed-out authentication requests.		
	<i>disable</i>	Disable logging timed-out authentication requests.		

config pac-policy

Parameter	Description	Type	Size	Default
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 forward-server

Configure forward-server addresses.

```
config web-proxy forward-server
  Description: Configure forward-server addresses.
  edit <name>
    set addr-type [ip|fqdn]
    set ip {ipv4-address-any}
    set fqdn {string}
    set port {integer}
    set healthcheck [disable|enable]
    set monitor {string}
    set server-down-option [block|pass]
    set username {string}
    set password {password}
    set comment {string}
  next
end
```

config web-proxy forward-server

Parameter	Description	Type	Size	Default
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option	Description		
	<i>ip</i>	Use an IP address for the forwarding proxy server.		
	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.		
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0
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 .	integer	Minimum value: 1 Maximum value: 65535	3128
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable health checking.		
	<i>enable</i>	Enable health checking.		
monitor	URL for forward server health check monitoring .	string	Maximum length: 255	http://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
	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	

Parameter	Description	Type	Size	Default
password	HTTP authentication password.	password	Not Specified	
comment	Comment.	string	Maximum length: 63	

config web-proxy forward-server-group

Configure a forward server group consisting or multiple forward servers. Supports failover and load balancing.

```
config web-proxy forward-server-group
    Description: Configure a forward server group consisting or 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
affinity	Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the forward-server-affinity-timeout is reached (under web-proxy global).	option	-	enable
Option				
enable				
disable				
ldb-method	Load balance method: weighted or least-session.	option	-	weighted
Option				
weighted				
least-session				

Parameter	Description	Type	Size	Default	
	Option	Description			
	<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	
	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
weight	Optionally assign a weight of the forwarding server for weighted load balancing	integer	Minimum value: 1 Maximum value: 100	10

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
url-pattern	URL exemption pattern.	string	Maximum length: 511	
status	Enable/disable this URL exemption.	option	-	enable

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	<i>enable</i>	Enable matching the exact path.		
	<i>disable</i>	Disable matching the exact path.		

config web-proxy wisp

Configure Wireless Internet service provider (WISP) servers.

```
config web-proxy wisp
  Description: Configure Wireless Internet service provider (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
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 .	integer	Minimum value: 1 Maximum value: 65535	15868

Parameter	Description	Type	Size	Default
max-connections	Maximum number of web proxy WISP connections .	integer	Minimum value: 4 Maximum value: 4096	64
timeout	Period of time before WISP requests time out .	integer	Minimum value: 1 Maximum value: 15	5

config web-proxy url-match

Exempt URLs from web proxy forwarding and caching.

```
config web-proxy url-match
  Description: Exempt URLs from web proxy forwarding and caching.
  edit <name>
    set status {enable|disable}
    set url-pattern {string}
    set forward-server {string}
    set cache-exemption {enable|disable}
    set comment {var-string}
  next
end
```

config web-proxy url-match

Parameter	Description	Type	Size	Default
status	Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding and caching.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable exempting the matching URLs.		
	<i>disable</i>	Disable exempting the matching URLs.		
url-pattern	URL pattern to be exempted from web proxy forwarding and caching.	string	Maximum length: 511	
forward-server	Forward server 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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable exempting this URL pattern from caching.		
comment	Comment.	var-string	Maximum length: 255	

webfilter

This section includes syntax for the following commands:

- config webfilter ips-urlfilter-setting on page 1527
 - config webfilter ips-urlfilter-cache-setting on page 1528
 - config webfilter ftgd-local-cat on page 1521
 - config webfilter content-header on page 1523
 - config webfilter override on page 1547
 - config webfilter ftgd-local-rating on page 1549
 - config webfilter profile on page 1529
 - config webfilter override-usr on page 1551
 - config webfilter fortiguard on page 1545
 - config webfilter search-engine on page 1549
 - config webfilter status on page 1550
 - config webfilter ips-urlfilter-setting6 on page 1528
 - config webfilter categories on page 1547
 - config webfilter urlfilter on page 1524
 - config webfilter content on page 1522
 - config webfilter ftgd-statistics on page 1550

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.			

Parameter	Description	Type	Size	Default
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0

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
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard
Option		Description		
<i>wildcard</i>		Wildcard pattern.		
<i>regexp</i>		Perl regular expression.		

Parameter	Description	Type	Size	Default
status	Enable/disable banned word.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
lang	Language of banned word.	option	-	western
	Option	Description		
	<i>western</i>	Western.		
	<i>simch</i>	Simplified Chinese.		
	<i>trach</i>	Traditional Chinese.		
	<i>japanese</i>	Japanese.		
	<i>korean</i>	Korean.		
	<i>french</i>	French.		
	<i>thai</i>	Thai.		
	<i>spanish</i>	Spanish.		
	<i>cyrillic</i>	Cyrillic.		
score	Score, to be applied every time the word appears on a web page .	integer	Minimum value: 0 Maximum value: 4294967295	10
action	Block or exempt word when a match is found.	option	-	block
	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
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
action	Action to take for this content type.	option	-	allow
Parameter	Description	Type	Size	Default
category	Categories that this content type applies to.	user	Not Specified	all

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]
        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
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.		
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable
	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.		

config entries

Parameter	Description	Type	Size	Default
url	URL to be filtered.	string	Maximum length: 511	
type	Filter type (simple, regex, or wildcard).	option	-	simple
	Option	Description		
	<i>simple</i>	Simple URL string.		
	<i>regex</i>	Regular expression URL string.		
	<i>wildcard</i>	Wildcard URL string.		
action	Action to take for URL filter matches.	option	-	exempt

Parameter	Description	Type	Size	Default
	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.		
	<i>pass</i>	Pass single connection from all.		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<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 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 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

Parameter	Description	Type	Size	Default
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

```
config webfilter ips-urlfilter-setting6
  Description: Configure IPS URL filter settings for IPv6.
  set device {string}
  set distance {integer}
  set gateway6 {ipv6-address}
  set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance 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 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. 0 means use DNS server's TTL	integer	Minimum value: 0 Maximum value: 2147483	0

config webfilter profile

Configure Web filter profiles.

```
config webfilter profile
  Description: Configure Web filter profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    set options {option1}, {option2}, ...
    set https-replacemsg [enable|disable]
    set ovrd-perm {option1}, {option2}, ...
    set post-action [normal|block]
    config override
      Description: Web Filter override settings.
      set ovrd-cookie [allow|deny]
      set ovrd-scope [user|user-group|...]
      set profile-type [list|radius]
      set ovrd-dur-mode [constant|ask]
      set ovrd-dur {user}
      set profile-attribute [User-Name|NAS-IP-Address|...]
      set ovrd-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 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 ovrd {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 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

```

```

        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 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 extended-log [enable|disable]
    set web-extended-all-action-log [enable|disable]
    set web-antiphishing-log [enable|disable]
next
end

```

config webfilter profile

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
feature-set	Flow/proxy feature set.	option	-	flow
Option		Description		
		flow Flow feature set.		
		proxy Proxy feature set.		
replacemsg-group	Replacement message group.	string	Maximum length: 35	
options	Options.	option	-	
Option		Description		
		activexfilter ActiveX filter.		
		cookiefilter Cookie filter.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>javafilter</i>	Java applet filter.		
	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.		
	<i>js</i>	Javascript 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.		
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ovrd-perm	Permitted override types.	option	-	
	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
	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

Parameter	Description	Type	Size	Default
	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.		
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 blocked web content.	option	-	enable
	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

Parameter	Description	Type	Size	Default
	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
	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-referer-log	Enable/disable logging referers.	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
	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

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
extended-log	Enable/disable extended logging for web filtering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-	disable
	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.		
	<i>user-group</i>	Override for the user's group.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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
	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
	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
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<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

Parameter	Description	Type	Size	Default														
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable setting.</td></tr> <tr> <td><i>disable</i></td><td>Disable setting.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
Option	Description																	
<i>enable</i>	Enable setting.																	
<i>disable</i>	Disable setting.																	
allowlist	FortiGuard allowlist settings.	option	-															
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>exempt-av</i></td><td>Exempt antivirus.</td></tr> <tr> <td><i>exempt-webcontent</i></td><td>Exempt web content.</td></tr> <tr> <td><i>exempt-activex-java-cookie</i></td><td>Exempt ActiveX-JAVA-Cookie.</td></tr> <tr> <td><i>exempt-dlp</i></td><td>Exempt DLP.</td></tr> <tr> <td><i>exempt-rangeblock</i></td><td>Exempt RangeBlock.</td></tr> <tr> <td><i>extended-log-others</i></td><td>Support extended log.</td></tr> </tbody> </table>					Option	Description	<i>exempt-av</i>	Exempt antivirus.	<i>exempt-webcontent</i>	Exempt web content.	<i>exempt-activex-java-cookie</i>	Exempt ActiveX-JAVA-Cookie.	<i>exempt-dlp</i>	Exempt DLP.	<i>exempt-rangeblock</i>	Exempt RangeBlock.	<i>extended-log-others</i>	Support extended log.
Option	Description																	
<i>exempt-av</i>	Exempt antivirus.																	
<i>exempt-webcontent</i>	Exempt web content.																	
<i>exempt-activex-java-cookie</i>	Exempt ActiveX-JAVA-Cookie.																	
<i>exempt-dlp</i>	Exempt DLP.																	
<i>exempt-rangeblock</i>	Exempt RangeBlock.																	
<i>extended-log-others</i>	Support extended log.																	
safe-search	Safe search type.	option	-															
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>url</i></td><td>Insert safe search string into URL.</td></tr> </tbody> </table>					Option	Description	<i>url</i>	Insert safe search string into URL.										
Option	Description																	
<i>url</i>	Insert safe search string into URL.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<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.		
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	**

** Values may differ between models.

config ftgd-wf

Parameter	Description	Type	Size	Default
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable
	Option	Description		
	<i>error-allow</i>	Allow web pages with a rating error to pass through.		
	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.		
	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.		
	<i>ftgd-disable</i>	Disable FortiGuard scanning.		
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17
ovrd	Allow web filter profile overrides.	user	Not Specified	

Parameter	Description	Type	Size	Default						
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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <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> </tbody> </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									
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0									
action	Action to take for matches.	option	-	monitor									
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>block</i></td><td>Block access.</td></tr> <tr> <td><i>authenticate</i></td><td>Authenticate user before allowing access.</td></tr> <tr> <td><i>monitor</i></td><td>Allow access while logging the action.</td></tr> <tr> <td><i>warning</i></td><td>Allow access after warning the user.</td></tr> </tbody> </table>	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.		
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.												

Parameter	Description	Type	Size	Default
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
Option	Description			
<i>session</i>	After session ends.			
<i>timeout</i>	After timeout occurs.			

config quota

Parameter	Description	Type	Size	Default
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
type	Quota type.	option	-	time
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

Parameter	Description	Type	Size	Default
	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.		
check-uri	Enable/disable checking of GET URI parameters for known credentials.	option	-	disable
	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.		

Parameter	Description	Type	Size	Default
check-basic-auth	Enable/disable checking of HTTP Basic Auth field for known credentials.	option	-	disable
	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
	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	65536
authentication	Authentication methods.	option	-	domain-controller
	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	
ldap	LDAP server for which to verify received credentials against.	string	Maximum length: 63	

config inspection-entries

Parameter	Description	Type	Size	Default
fortiguard-category	FortiGuard category to match.	user	Not Specified	g21
action	Action to be taken upon an AntiPhishing match.	option	-	exempt

Parameter	Description	Type	Size	Default
	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
category	Category that the pattern matches.	option	-	username
	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
	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 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-percent {integer}
  set ovrd-auth-port-http {integer}
  set ovrd-auth-port-https {integer}
  set ovrd-auth-port-https-flow {integer}
  set ovrd-auth-port-warning {integer}
  set ovrd-auth-https [enable|disable]
  set warn-auth-https [enable|disable]
  set close-ports [enable|disable]
    set request-packet-size-limit {integer}
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-percent	Maximum percentage of available memory allocated to caching .	integer	Minimum value: 1 Maximum value: 15	2 **
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication	integer	Minimum value: 0 Maximum value: 65535	8008
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable

Parameter	Description	Type	Size	Default
	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
	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
	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 .	integer	Minimum value: 576 Maximum value: 10000	0

** Values may differ between models.

config webfilter categories

List the FortiGuard Web Filter category descriptions.

```
config webfilter categories
    Description: List the FortiGuard Web Filter category descriptions.
end
```

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		
	Option	Description					
status	enable	Enable override rule.	option	-	disable		
	disable	Disable override rule.					
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.		option	-	user		
	user	Override the specified user.					
ip	user-group	Override the specified user group.	ipv4-address	Not Specified	0.0.0.0		
	ip	Override the specified IP address.					
	ip6	Override the specified IPv6 address.					
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 17:00:00			
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64				

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
status	Enable/disable local rating.	option	-	enable
Parameter	Description	Option	-	enable
		enable		Enable local rating.
		disable		Disable local rating.
comment	Comment.	var-string	Maximum length: 255	
rating	Local rating.	user	Not Specified	

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 safesearch-str {string}
    next
end
```

config webfilter search-engine

Parameter	Description	Type	Size	Default
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).			
charset	Search engine charset.	option	-	utf-8
Option	Description			
<i>utf-8</i>	UTF-8 encoding.			
<i>gb2312</i>	GB2312 encoding.			
safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79	

config webfilter ftgd-statistics

Display rating cache and daemon statistics.

```
config webfilter ftgd-statistics
  Description: Display rating cache and daemon statistics.
end
```

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: -1	

config webfilter override-usr

Display list of user overrides.

```
config webfilter override-usr
    Description: Display list of user overrides.
end
```

wireless-controller

This section includes syntax for the following commands:

- [config wireless-controller address](#) on page 1738
- [config wireless-controller setting](#) on page 1609
- [config wireless-controller status](#) on page 1748
- [config wireless-controller hotspot20 hs-profile](#) on page 1572
- [config wireless-controller wids-profile](#) on page 1629
- [config wireless-controller client-info](#) on page 1749
- [config wireless-controller hotspot20 h2qp-wan-metric](#) on page 1564
- [config wireless-controller hotspot20 h2qp-conn-capability](#) on page 1566
- [config wireless-controller hotspot20 anqp-venue-name](#) on page 1557
- [config wireless-controller mpsk-profile](#) on page 1742
- [config wireless-controller wtp-status](#) on page 1749
- [config wireless-controller region](#) on page 1628
- [config wireless-controller global](#) on page 1554
- [config wireless-controller utm-profile](#) on page 1737
- [config wireless-controller wtp-group](#) on page 1729
- [config wireless-controller nac-profile](#) on page 1744
- [config wireless-controller log](#) on page 1618
- [config wireless-controller wag-profile](#) on page 1735
- [config wireless-controller hotspot20 anqp-3gpp-cellular](#) on page 1562
- [config wireless-controller hotspot20 h2qp-operator-name](#) on page 1564
- [config wireless-controller vap-status](#) on page 1749
- [config wireless-controller timers](#) on page 1607
- [config wireless-controller rf-analysis](#) on page 1750
- [config wireless-controller wtp-profile](#) on page 1638
- [config wireless-controller hotspot20 icon](#) on page 1568
- [config wireless-controller hotspot20 anqp-roaming-consortium](#) on page 1559
- [config wireless-controller qos-profile](#) on page 1732
- [config wireless-controller hotspot20 anqp-network-auth-type](#) on page 1558
- [config wireless-controller spectral-info](#) on page 1750
- [config wireless-controller inter-controller](#) on page 1553
- [config wireless-controller hotspot20 qos-map](#) on page 1571
- [config wireless-controller ble-profile](#) on page 1636
- [config wireless-controller vap-group](#) on page 1629
- [config wireless-controller hotspot20 h2qp-osu-provider](#) on page 1569
- [config wireless-controller access-control-list](#) on page 1745
- [config wireless-controller apcfg-profile](#) on page 1623
- [config wireless-controller scan](#) on page 1747
- [config wireless-controller arrp-profile](#) on page 1625
- [config wireless-controller wtp](#) on page 1707

- [config wireless-controller hotspot20 anqp-ip-address-type](#) on page 1563
- [config wireless-controller vap](#) on page 1579
- [config wireless-controller snmp](#) on page 1739
- [config wireless-controller hotspot20 anqp-nai-realm](#) on page 1559
- [config wireless-controller wlchanlistic](#) on page 1748
- [config wireless-controller ssid-policy](#) on page 1745
- [config wireless-controller bonjour-profile](#) on page 1624
- [config wireless-controller ap-status](#) on page 1747
- [config wireless-controller addrgrp](#) on page 1738

config wireless-controller inter-controller

Configure inter wireless controller operation.

```
config wireless-controller inter-controller
    Description: Configure inter wireless controller operation.
    set inter-controller-mode {disable|l2-roaming|...}
    set inter-controller-key {password}
    set inter-controller-pri {primary|secondary}
    set fast-failover-max {integer}
    set fast-failover-wait {integer}
    config inter-controller-peer
        Description: Fast failover peer wireless controller list.
        edit <id>
            set peer-ip {ipv4-address}
            set peer-port {integer}
            set peer-priority {primary|secondary}
        next
    end
end
```

config wireless-controller inter-controller

Parameter	Description	Type	Size	Default
inter-controller-mode	Configure inter-controller mode .	option	-	disable
Option				
disable				
Disable inter-controller mode.				
l2-roaming				
Enable layer 2 roaming support between inter-controllers.				
1+1				
Enable 1+1 fast failover mode.				
inter-controller-key	Secret key for inter-controller communications.	password	Not Specified	

Parameter	Description	Type	Size	Default
inter-controller-pri	Configure inter-controller's priority .	option	-	primary
	Option	Description		
	<i>primary</i>	Primary fast failover mode.		
	<i>secondary</i>	Secondary fast failover mode.		
fast-failover-max	Maximum number of retransmissions for fast failover HA messages between peer wireless controllers .	integer	Minimum value: 3 Maximum value: 64	10
fast-failover-wait	Minimum wait time before an AP transitions from secondary controller to primary controller .	integer	Minimum value: 10 Maximum value: 86400	10

config inter-controller-peer

Parameter	Description	Type	Size	Default
peer-ip	Peer wireless controller's IP address.	ipv4-address	Not Specified	0.0.0.0
peer-port	Port used by the wireless controller's for inter-controller communications .	integer	Minimum value: 1024 Maximum value: 49150	5246
peer-priority	Peer wireless controller's priority .	option	-	primary
	Option	Description		
	<i>primary</i>	Primary fast failover mode.		
	<i>secondary</i>	Secondary fast failover mode.		

config wireless-controller global

Configure wireless controller global settings.

```
config wireless-controller global
  Description: Configure wireless controller global settings.
  set name {string}
  set location {string}
  set image-download [enable|disable]
  set max-retransmit {integer}
  set control-message-offload {option1}, {option2}, ...
```

```

set data-ethernet-II [enable|disable]
set link-aggregation [enable|disable]
set mesh-eth-type {integer}
set fiapp-eth-type {integer}
set discovery-mc-addr {ipv4-address-multicast}
set max-clients {integer}
set rogue-scan-mac-adjacency {integer}
set ipsec-base-ip {ipv4-address}
set wtp-share [enable|disable]
set tunnel-mode [compatible|strict]
set ap-log-server [enable|disable]
set ap-log-server-ip {ipv4-address}
set ap-log-server-port {integer}
end

```

config wireless-controller global

Parameter	Description	Type	Size	Default
name	Name of the wireless controller.	string	Maximum length: 35	
location	Description of the location of the wireless controller.	string	Maximum length: 35	
image-download	Enable/disable WTP image download at join time.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable WTP image download at join time.		
	<i>disable</i>	Disable WTP image download at join time.		
max-retransmit	Maximum number of tunnel packet retransmissions .	integer	Minimum value: 0 Maximum value: 64	3
control-message-offload	Configure CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis
	Option	Description		
	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.		

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>aeroscout-tag</i></td><td>AeroScout tag.</td></tr> <tr> <td><i>ap-list</i></td><td>Rogue AP list.</td></tr> <tr> <td><i>sta-list</i></td><td>Rogue STA list.</td></tr> <tr> <td><i>sta-cap-list</i></td><td>STA capability list.</td></tr> <tr> <td><i>stats</i></td><td>WTP, radio, VAP, and STA statistics.</td></tr> <tr> <td><i>aeroscout-mu</i></td><td>AeroScout Mobile Unit (MU) report.</td></tr> <tr> <td><i>sta-health</i></td><td>STA health log.</td></tr> <tr> <td><i>spectral-analysis</i></td><td>Spectral analysis report.</td></tr> </tbody> </table>	Option	Description	<i>aeroscout-tag</i>	AeroScout tag.	<i>ap-list</i>	Rogue AP list.	<i>sta-list</i>	Rogue STA list.	<i>sta-cap-list</i>	STA capability list.	<i>stats</i>	WTP, radio, VAP, and STA statistics.	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	<i>sta-health</i>	STA health log.	<i>spectral-analysis</i>	Spectral analysis report.			
Option	Description																					
<i>aeroscout-tag</i>	AeroScout tag.																					
<i>ap-list</i>	Rogue AP list.																					
<i>sta-list</i>	Rogue STA list.																					
<i>sta-cap-list</i>	STA capability list.																					
<i>stats</i>	WTP, radio, VAP, and STA statistics.																					
<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.																					
<i>sta-health</i>	STA health log.																					
<i>spectral-analysis</i>	Spectral analysis report.																					
data-ethernet-II	Configure the wireless controller to use Ethernet II option or 802.3 frames with 802.3 data tunnel mode .	-	-	enable																		
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Use Ethernet II frames with 802.3 data tunnel mode.</td></tr> <tr> <td><i>disable</i></td><td>Use 802.3 Ethernet frames with 802.3 data tunnel mode.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.	<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.															
Option	Description																					
<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.																					
<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.																					
link-aggregation	Enable/disable calculating the CAPWAP transmit hash to load balance sessions to link aggregation nodes .	option	-	disable																		
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable calculating the CAPWAP transmit hash.</td></tr> <tr> <td><i>disable</i></td><td>Disable calculating the CAPWAP transmit hash.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable calculating the CAPWAP transmit hash.	<i>disable</i>	Disable calculating the CAPWAP transmit hash.															
Option	Description																					
<i>enable</i>	Enable calculating the CAPWAP transmit hash.																					
<i>disable</i>	Disable calculating the CAPWAP transmit hash.																					
mesh-eth-type	Mesh Ethernet identifier included in backhaul packets .	integer	Minimum value: 0 Maximum value: 65535	8755																		
fiapp-eth-type	Ethernet type for Fortinet Inter-Access Point Protocol .	integer	Minimum value: 0 Maximum value: 65535	5252																		
discovery-mc-addr	Multicast IP address for AP discovery .	ipv4-address-multicast	Not Specified	224.0.1.140																		

Parameter	Description	Type	Size	Default
max-clients	Maximum number of clients that can connect simultaneously .	integer	Minimum value: 0 Maximum value: 4294967295	0
rogue-scan-mac-adjacency	Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection .	integer	Minimum value: 0 Maximum value: 31	7
ipsec-base-ip	Base IP address for IPsec VPN tunnels between the access points and the wireless controller .	ipv4-address	Not Specified	169.254.0.1
wtp-share	Enable/disable sharing of WTPs between VDOMs.	option	-	disable
Option	Description			
<i>enable</i>	WTP can be shared between all VDOMs.			
<i>disable</i>	WTP can be used only in its own VDOM.			
tunnel-mode	Compatible/strict tunnel mode.	option	-	compatible
Option	Description			
<i>compatible</i>	Allow for backward compatible ciphers(3DES+SHA1+Strong list).			
<i>strict</i>	Follow system level strong-crypto ciphers.			
ap-log-server	Enable/disable configuring APs or FortiAPs to send log messages to a syslog server .	option	-	disable
Option	Description			
<i>enable</i>	Enable AP log server.			
<i>disable</i>	Disable AP log server.			
ap-log-server-ip	IP address that APs or FortiAPs send log messages to.	ipv4-address	Not Specified	0.0.0.0
ap-log-server-port	Port that APs or FortiAPs send log messages to.	integer	Minimum value: 0 Maximum value: 65535	0

config wireless-controller hotspot20 anqp-venue-name

Configure venue name duple.

```
config wireless-controller hotspot20 anqp-venue-name
```

```

Description: Configure venue name duple.
edit <name>
    config value-list
        Description: Name list.
        edit <index>
            set lang {string}
            set value {string}
        next
    end
next
end

```

config value-list

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
value	Venue name value.	string	Maximum length: 252	

config wireless-controller hotspot20 anqp-network-auth-type

Configure network authentication type.

```

config wireless-controller hotspot20 anqp-network-auth-type
    Description: Configure network authentication type.
    edit <name>
        set auth-type [acceptance-of-terms|online-enrollment|...]
        set url {string}
    next
end

```

config wireless-controller hotspot20 anqp-network-auth-type

Parameter	Description	Type	Size	Default
auth-type	Network authentication type.	option	-	acceptance-of-terms
Option	Description			
<i>acceptance-of-terms</i>	Acceptance of terms and conditions.			
<i>online-enrollment</i>	Online enrollment supported.			
<i>http-redirection</i>	HTTP and HTTPS redirection.			
<i>dns-redirection</i>	DNS redirection.			
url	Redirect URL.	string	Maximum length: 255	

config wireless-controller hotspot20 anqp-roaming-consortium

Configure roaming consortium.

```
config wireless-controller hotspot20 anqp-roaming-consortium
    Description: Configure roaming consortium.
    edit <name>
        config oi-list
            Description: Organization identifier list.
            edit <index>
                set oi {string}
                set comment {string}
            next
        end
    next
end
```

config oi-list

Parameter	Description	Type	Size	Default
oi	Organization identifier.	string	Maximum length: 10	
comment	Comment.	string	Maximum length: 35	

config wireless-controller hotspot20 anqp-nai-realm

Configure network access identifier (NAI) realm.

```
config wireless-controller hotspot20 anqp-nai-realm
    Description: Configure network access identifier (NAI) realm.
    edit <name>
        config nai-list
            Description: NAI list.
            edit <name>
                set encoding [disable|enable]
                set nai-realm {string}
                config eap-method
                    Description: EAP Methods.
                    edit <index>
                        set method [eap-identity|eap-md5|...]
                        config auth-param
                            Description: EAP auth param.
                            edit <index>
                                set id [non-eap-inner-auth|inner-auth-eap|...]
                                set val [eap-identity|eap-md5|...]
                            next
                        end
                    next
                end
            next
        end
    next
end
```

end

config nai-list

Parameter	Description	Type	Size	Default
encoding	Enable/disable format in accordance with IETF RFC 4282.	option	-	enable
Option	Description			
<i>disable</i>				Disable format in accordance with IETF RFC 4282.
<i>enable</i>				Enable format in accordance with IETF RFC 4282.
nai-realm	Configure NAI realms (delimited by a semi-colon character).	string	Maximum length: 255	

config eap-method

Parameter	Description	Type	Size	Default
method	EAP method type.	option	-	eap-identity
Option	Description			
<i>eap-identity</i>				Identity.
<i>eap-md5</i>				MD5.
<i>eap-tls</i>				TLS.
<i>eap-ttls</i>				TTLS.
<i>eap-peap</i>				PEAP.
<i>eap-sim</i>				SIM.
<i>eap-aka</i>				AKA.
<i>eap-aka-prime</i>				AKA'.

config auth-param

Parameter	Description	Type	Size	Default
id	ID of authentication parameter.	option	-	inner-auth-eap
Option	Description			
<i>non-eap-inner-auth</i>				Non-EAP inner authentication type.

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>inner-auth-eap</i>	Inner authentication EAP method type.		
	<i>credential</i>	Credential type.		
	<i>tunneled-credential</i>	Tunneled EAP method credential type.		
val	Value of authentication parameter.	option	-	eap-identity
	Option	Description		
	<i>eap-identity</i>	EAP Identity.		
	<i>eap-md5</i>	EAP MD5.		
	<i>eap-tls</i>	EAP TLS.		
	<i>eap-ttls</i>	EAP TTLS.		
	<i>eap-peap</i>	EAP PEAP.		
	<i>eap-sim</i>	EAP SIM.		
	<i>eap-aka</i>	EAP AKA.		
	<i>eap-aka-prime</i>	EAP AKA'.		
	<i>non-eap-pap</i>	Non EAP PAP.		
	<i>non-eap-chap</i>	Non EAP CHAP.		
	<i>non-eap-mschap</i>	Non EAP MSCHAP.		
	<i>non-eap-mschapv2</i>	Non EAP MSCHAPV2.		
	<i>cred-sim</i>	Credential SIM.		
	<i>cred-usim</i>	Credential USIM.		
	<i>cred-nfc</i>	Credential NFC secure element.		
	<i>cred-hardware-token</i>	Credential hardware token.		
	<i>cred-softoken</i>	Credential softtoken.		
	<i>cred-certificate</i>	Credential certificate.		
	<i>cred-user-pwd</i>	Credential username password.		
	<i>cred-none</i>	Credential none.		

Parameter	Description	Type	Size	Default
Option	Description			
<i>cred-vendor-specific</i>	Credential vendor specific.			
<i>tun-cred-sim</i>	Tunneled credential SIM.			
<i>tun-cred-usim</i>	Tunneled credential USIM.			
<i>tun-cred-nfc</i>	Tunneled credential NFC secure element.			
<i>tun-cred-hardware-token</i>	Tunneled credential hardware token.			
<i>tun-cred-softoken</i>	Tunneled credential softtoken.			
<i>tun-cred-certificate</i>	Tunneled credential certificate.			
<i>tun-cred-user-pwd</i>	Tunneled credential username password.			
<i>tun-cred-anonymous</i>	Tunneled credential anonymous.			
<i>tun-cred-vendor-specific</i>	Tunneled credential vendor specific.			

config wireless-controller hotspot20 anqp-3gpp-cellular

Configure 3GPP public land mobile network (PLMN).

```
config wireless-controller hotspot20 anqp-3gpp-cellular
  Description: Configure 3GPP public land mobile network (PLMN) .
  edit <name>
    config mcc-mnc-list
      Description: Mobile Country Code and Mobile Network Code configuration.
      edit <id>
        set mcc {string}
        set mnc {string}
      next
    end
  next
end
```

config mcc-mnc-list

Parameter	Description	Type	Size	Default
mcc	Mobile country code.	string	Maximum length: 3	

Parameter	Description	Type	Size	Default
mnc	Mobile network code.	string	Maximum length: 3	

config wireless-controller hotspot20 anqp-ip-address-type

Configure IP address type availability.

```
config wireless-controller hotspot20 anqp-ip-address-type
  Description: Configure IP address type availability.
  edit <name>
    set ipv6-address-type [not-available|available|...]
    set ipv4-address-type [not-available|public|...]
  next
end
```

config wireless-controller hotspot20 anqp-ip-address-type

Parameter	Description	Type	Size	Default
ipv6-address-type	IPv6 address type.	option	-	not-available
Option		Description		
<i>not-available</i>		Address type not available.		
<i>available</i>		Address type available.		
<i>not-known</i>		Availability of the address type not known.		
ipv4-address-type	IPv4 address type.	option	-	not-available
Option		Description		
<i>not-available</i>		Address type not available.		
<i>public</i>		Public IPv4 address available.		
<i>port-restricted</i>		Port-restricted IPv4 address available.		
<i>single-NATed-private</i>		Single NATed private IPv4 address available.		
<i>double-NATed-private</i>		Double NATed private IPv4 address available.		
<i>port-restricted-and-single-NATed</i>		Port-restricted IPv4 address and single NATed IPv4 address available.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.		
	<i>not-known</i>	Availability of the address type is not known.		

config wireless-controller hotspot20 h2qp-operator-name

Configure operator friendly name.

```
config wireless-controller hotspot20 h2qp-operator-name
    Description: Configure operator friendly name.
    edit <name>
        config value-list
            Description: Name list.
            edit <index>
                set lang {string}
                set value {string}
            next
        end
    next
end
```

config value-list

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
value	Friendly name value.	string	Maximum length: 252	

config wireless-controller hotspot20 h2qp-wan-metric

Configure WAN metrics.

```
config wireless-controller hotspot20 h2qp-wan-metric
    Description: Configure WAN metrics.
    edit <name>
        set link-status [up|down|...]
        set symmetric-wan-link [symmetric|asymmetric]
        set link-at-capacity [enable|disable]
        set uplink-speed {integer}
        set downlink-speed {integer}
        set uplink-load {integer}
        set downlink-load {integer}
        set load-measurement-duration {integer}
    next
end
```

config wireless-controller hotspot20 h2qp-wan-metric

Parameter	Description	Type	Size	Default								
link-status	Link status.	option	-	up								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>up</i></td><td>Link up.</td></tr> <tr> <td><i>down</i></td><td>Link down.</td></tr> <tr> <td><i>in-test</i></td><td>Link in test state.</td></tr> </tbody> </table>	Option	Description	<i>up</i>	Link up.	<i>down</i>	Link down.	<i>in-test</i>	Link in test state.			
Option	Description											
<i>up</i>	Link up.											
<i>down</i>	Link down.											
<i>in-test</i>	Link in test state.											
symmetric-wan-link	WAN link symmetry.	option	-	asymmetric								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>symmetric</i></td><td>Symmetric WAN link (uplink and downlink speeds are the same).</td></tr> <tr> <td><i>asymmetric</i></td><td>Asymmetric WAN link (uplink and downlink speeds are not the same).</td></tr> </tbody> </table>	Option	Description	<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).	<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).					
Option	Description											
<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).											
<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).											
link-at-capacity	Link at capacity.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Link at capacity (not allow additional mobile devices to associate).</td></tr> <tr> <td><i>disable</i></td><td>Link not at capacity (allow additional mobile devices to associate).</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).	<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).					
Option	Description											
<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).											
<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).											
uplink-speed	Uplink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295	2400								
downlink-speed	Downlink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295	2400								
uplink-load	Uplink load.	integer	Minimum value: 0 Maximum value: 255	0								
downlink-load	Downlink load.	integer	Minimum value: 0 Maximum value: 255	0								

Parameter	Description	Type	Size	Default
load-measurement-duration	Load measurement duration (in tenths of a second).	integer	Minimum value: 0 Maximum value: 65535	0

config wireless-controller hotspot20 h2qp-conn-capability

Configure connection capability.

```
config wireless-controller hotspot20 h2qp-conn-capability
  Description: Configure connection capability.
  edit <name>
    set icmp-port [closed|open|...]
    set ftp-port [closed|open|...]
    set ssh-port [closed|open|...]
    set http-port [closed|open|...]
    set tls-port [closed|open|...]
    set pptp-vpn-port [closed|open|...]
    set voip-tcp-port [closed|open|...]
    set voip-udp-port [closed|open|...]
    set ikev2-port [closed|open|...]
    set ikev2-xx-port [closed|open|...]
    set esp-port [closed|open|...]
  next
end
```

config wireless-controller hotspot20 h2qp-conn-capability

Parameter	Description	Type	Size	Default
icmp-port	Set ICMP port service status.	option	-	unknown
Option		Description		
<i>closed</i>		The port is not open for communication.		
<i>open</i>		The port is open for communication.		
<i>unknown</i>		The port may or may not be open for communication.		
ftp-port	Set FTP port service status.	option	-	unknown
Option		Description		
<i>closed</i>		The port is not open for communication.		
<i>open</i>		The port is open for communication.		
<i>unknown</i>		The port may or may not be open for communication.		
ssh-port	Set SSH port service status.	option	-	unknown

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
http-port	Set HTTP port service status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
tls-port	Set TLS VPN (HTTPS) port service status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
pptp-vpn-port	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
voip-tcp-port	Set VoIP TCP port service status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
voip-udp-port	Set VoIP UDP port service status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
ikev2-port	Set IKEv2 port service for IPsec VPN status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
ikev2-xx-port	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
esp-port	Set ESP port service (used by IPsec VPNs) status.	option	-	unknown
	Option	Description		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		

config wireless-controller hotspot20 icon

Configure OSU provider icon.

```
config wireless-controller hotspot20 icon
  Description: Configure OSU provider icon.
  edit <name>
    config icon-list
      Description: Icon list.
      edit <name>
        set lang {string}
        set file {string}
        set type [bmp|gif|...]
        set width {integer}
        set height {integer}
      next
    end
  next
```

```
end
```

config icon-list

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
file	Icon file.	string	Maximum length: 255	
type	Icon type.	option	-	png
Option		Description		
		<i>bmp</i> BMP image.		
		<i>gif</i> GIF image.		
		<i>jpeg</i> JPEG image.		
		<i>png</i> PNG image.		
		<i>tiff</i> TIFF image.		
width	Icon width.	integer	Minimum value: 1 Maximum value: 65535	0
height	Icon height.	integer	Minimum value: 1 Maximum value: 65535	0

config wireless-controller hotspot20 h2qp-osu-provider

Configure online sign up (OSU) provider list.

```
config wireless-controller hotspot20 h2qp-osu-provider
  Description: Configure online sign up (OSU) provider list.
  edit <name>
    config friendly-name
      Description: OSU provider friendly name.
      edit <index>
        set lang {string}
        set friendly-name {string}
      next
    end
    set server-uri {string}
    set osu-method {option1}, {option2}, ...
    set osu-nai {string}
    config service-description
```

```

Description: OSU service name.
edit <service-id>
    set lang {string}
    set service-description {string}
next
end
set icon {string}
next
end

```

config wireless-controller hotspot20 h2qp-osu-provider

Parameter	Description	Type	Size	Default
server-uri	Server URI.	string	Maximum length: 255	
	Option	Description		
	<i>oma-dm</i>	OMA DM.		
	<i>soap-xml-spp</i>	SOAP XML SPP.		
	<i>reserved</i>	Reserved.		
osu-nai	OSU NAI.	string	Maximum length: 255	
icon	OSU provider icon.	string	Maximum length: 35	

config friendly-name

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
friendly-name	OSU provider friendly name.	string	Maximum length: 252	

config service-description

Parameter	Description	Type	Size	Default
lang	Language code.	string	Maximum length: 3	eng
service-description	Service description.	string	Maximum length: 252	

config wireless-controller hotspot20 qos-map

Configure QoS map set.

```
config wireless-controller hotspot20 qos-map
    Description: Configure QoS map set.
    edit <name>
        config dscp-except
            Description: Differentiated Services Code Point (DSCP) exceptions.
            edit <index>
                set dscp {integer}
                set up {integer}
            next
        end
        config dscp-range
            Description: Differentiated Services Code Point (DSCP) ranges.
            edit <index>
                set up {integer}
                set low {integer}
                set high {integer}
            next
        end
    next
end
```

config dscp-except

Parameter	Description	Type	Size	Default
dscp	DSCP value.	integer	Minimum value: 0 Maximum value: 63	0
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0

config dscp-range

Parameter	Description	Type	Size	Default
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0
low	DSCP low value.	integer	Minimum value: 0 Maximum value: 63	255

Parameter	Description	Type	Size	Default
high	DSCP high value.	integer	Minimum value: 0 Maximum value: 63	255

config wireless-controller hotspot20 hs-profile

Configure hotspot profile.

```
config wireless-controller hotspot20 hs-profile
  Description: Configure hotspot profile.
  edit <name>
    set access-network-type [private-network|private-network-with-guest-access|...]
    set access-network-internet [enable|disable]
    set access-network-asra [enable|disable]
    set access-network-esr [enable|disable]
    set access-network-uesa [enable|disable]
    set venue-group [unspecified|assembly|...]
    set venue-type [unspecified|arena|...]
    set hessid {mac-address}
    set proxy-arp [enable|disable]
    set 12tif [enable|disable]
    set pame-bi [disable|enable]
    set anqp-domain-id {integer}
    set domain-name {string}
    set osu-ssid {string}
    set gas-comeback-delay {integer}
    set gas-fragmentation-limit {integer}
    set dgaf [enable|disable]
    set deauth-request-timeout {integer}
    set wnm-sleep-mode [enable|disable]
    set bss-transition [enable|disable]
    set venue-name {string}
    set roaming-consortium {string}
    set nai-realm {string}
    set oper-friendly-name {string}
    set osu-provider <name1>, <name2>, ...
    set wan-metrics {string}
    set network-auth {string}
    set 3gpp-plmn {string}
    set conn-cap {string}
    set qos-map {string}
    set ip-addr-type {string}
  next
end
```

config wireless-controller hotspot20 hs-profile

Parameter	Description	Type	Size	Default
access-network-type	Access network type.	option	-	private-network
	Option	Description		
	<i>private-network</i>	Private network.		
	<i>private-network-with-guest-access</i>	Private network with guest access.		
	<i>chargeable-public-network</i>	Chargeable public network.		
	<i>free-public-network</i>	Free public network.		
	<i>personal-device-network</i>	Personal devices network.		
	<i>emergency-services-only-network</i>	Emergency services only network.		
	<i>test-or-experimental</i>	Test or experimental.		
	<i>wildcard</i>	Wildcard.		
access-network-internet	Enable/disable connectivity to the Internet.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable connectivity to the Internet.		
	<i>disable</i>	Disable connectivity to the Internet.		
access-network-asra	Enable/disable additional step required for access (ASRA).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable additional step required for access (ASRA).		
	<i>disable</i>	Disable additional step required for access (ASRA).		
access-network-esr	Enable/disable emergency services reachable (ESR).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable emergency services reachable (ESR).		
	<i>disable</i>	Disable emergency services reachable (ESR).		
access-network-uesa	Enable/disable unauthenticated emergency service accessible (UESA).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).		
	<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).		
venue-group	Venue group.	option	-	unspecified
	Option	Description		
	<i>unspecified</i>	Unspecified.		
	<i>assembly</i>	Assembly.		
	<i>business</i>	Business.		
	<i>educational</i>	Educational.		
	<i>factory</i>	Factory and industrial.		
	<i>institutional</i>	Institutional.		
	<i>mercantile</i>	Mercantile.		
	<i>residential</i>	Residential.		
	<i>storage</i>	Storage.		
	<i>utility</i>	Utility and miscellaneous.		
	<i>vehicular</i>	Vehicular.		
	<i>outdoor</i>	Outdoor.		
venue-type	Venue type.	option	-	unspecified
	Option	Description		
	<i>unspecified</i>	Unspecified.		
	<i>arena</i>	Arena.		
	<i>stadium</i>	Stadium.		
	<i>passenger-terminal</i>	Passenger terminal.		

Parameter	Description	Type	Size	Default
Option	Description			
<i>amphitheater</i>	Amphitheater.			
<i>amusement-park</i>	Amusement park.			
<i>place-of-worship</i>	Place of worship.			
<i>convention-center</i>	Convention center.			
<i>library</i>	Library.			
<i>museum</i>	Museum.			
<i>restaurant</i>	Restaurant.			
<i>theater</i>	Theater.			
<i>bar</i>	Bar.			
<i>coffee-shop</i>	Coffee shop.			
<i>zoo-or-aquarium</i>	Zoo or aquarium.			
<i>emergency-center</i>	Emergency coordination center.			
<i>doctor-office</i>	Doctor or dentist office.			
<i>bank</i>	Bank.			
<i>fire-station</i>	Fire station.			
<i>police-station</i>	Police station.			
<i>post-office</i>	Post office.			
<i>professional-office</i>	Professional office.			
<i>research-facility</i>	Research and development facility.			
<i>attorney-office</i>	Attorney office.			
<i>primary-school</i>	Primary school.			
<i>secondary-school</i>	Secondary school.			
<i>university-or-college</i>	University or college.			
<i>factory</i>	Factory.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>hospital</i>	Hospital.		
	<i>long-term-care-facility</i>	Long term care facility.		
	<i>rehab-center</i>	Alcohol and drug rehabilitation center.		
	<i>group-home</i>	Group home.		
	<i>prison-or-jail</i>	Prison or jail.		
	<i>retail-store</i>	Retail store.		
	<i>grocery-market</i>	Grocery market.		
	<i>auto-service-station</i>	Auto service station.		
	<i>shopping-mall</i>	Shopping mall.		
	<i>gas-station</i>	Gas station.		
	<i>private</i>	Private residence.		
	<i>hotel-or-motel</i>	Hotel or motel.		
	<i>dormitory</i>	Dormitory.		
	<i>boarding-house</i>	Boarding house.		
	<i>automobile</i>	Automobile or truck.		
	<i>airplane</i>	Airplane.		
	<i>bus</i>	Bus.		
	<i>ferry</i>	Ferry.		
	<i>ship-or-boat</i>	Ship or boat.		
	<i>train</i>	Train.		
	<i>motor-bike</i>	Motor bike.		
	<i>muni-mesh-network</i>	Muni mesh network.		
	<i>city-park</i>	City park.		
	<i>rest-area</i>	Rest area.		
	<i>traffic-control</i>	Traffic control.		
	<i>bus-stop</i>	Bus stop.		
	<i>kiosk</i>	Kiosk.		

Parameter	Description	Type	Size	Default
hessid	Homogeneous extended service set identifier (HESSID).	mac-address	Not Specified	00:00:00:00:00:00
proxy-arp	Enable/disable Proxy ARP.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Proxy ARP.		
	<i>disable</i>	Disable Proxy ARP.		
l2tif	Enable/disable Layer 2 traffic inspection and filtering.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Layer 2 traffic inspection and filtering.		
	<i>disable</i>	Disable Layer 2 traffic inspection and filtering.		
pame-bi	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).		
	<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).		
anqp-domain-id	ANQP Domain ID .	integer	Minimum value: 0 Maximum value: 65535	0
domain-name	Domain name.	string	Maximum length: 255	
osu-ssid	Online sign up (OSU) SSID.	string	Maximum length: 255	
gas-comeback-delay	GAS comeback delay .	integer	Minimum value: 100 Maximum value: 10000	500

Parameter	Description	Type	Size	Default
gas-fragmentation-limit	GAS fragmentation limit .	integer	Minimum value: 512 Maximum value: 4096	1024
dgaf	Enable/disable downstream group-addressed forwarding (DGAf).	option	-	disable
Option		Description		
		<i>enable</i> Enable downstream group-addressed forwarding (DGAf).		
		<i>disable</i> Disable downstream group-addressed forwarding (DGAf).		
deauth-request-timeout	Deauthentication request timeout (in seconds).	integer	Minimum value: 30 Maximum value: 120	60
wnm-sleep-mode	Enable/disable wireless network management (WNM) sleep mode.	option	-	disable
Option		Description		
		<i>enable</i> Enable wireless network management (WNM) sleep mode.		
		<i>disable</i> Disable wireless network management (WNM) sleep mode.		
bss-transition	Enable/disable basic service set (BSS) transition Support.	option	-	disable
Option		Description		
		<i>enable</i> Enable basic service set (BSS) transition support.		
		<i>disable</i> Disable basic service set (BSS) transition support.		
venue-name	Venue name.	string	Maximum length: 35	
roaming-consortium	Roaming consortium list name.	string	Maximum length: 35	
nai-realm	NAI realm list name.	string	Maximum length: 35	
oper-friendly-name	Operator friendly name.	string	Maximum length: 35	
osu-provider <name>	Manually selected list of OSU provider(s). OSU provider name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
wan-metrics	WAN metric name.	string	Maximum length: 35	
network-auth	Network authentication name.	string	Maximum length: 35	
3gpp-plmn	3GPP PLMN name.	string	Maximum length: 35	
conn-cap	Connection capability name.	string	Maximum length: 35	
qos-map	QoS MAP set ID.	string	Maximum length: 35	
ip-addr-type	IP address type name.	string	Maximum length: 35	

config wireless-controller vap

Configure Virtual Access Points (VAPs).

```
config wireless-controller vap
  Description: Configure Virtual Access Points (VAPs).
  edit <name>
    set fast-roaming {enable|disable}
    set external-fast-roaming {enable|disable}
    set mesh-backhaul {enable|disable}
    set atf-weight {integer}
    set max-clients {integer}
    set max-clients-ap {integer}
    set ssid {string}
    set broadcast-ssid {enable|disable}
    set security {open|captive-portal|...}
    set pmf {disable|enable|...}
    set pmf-assoc-comeback-timeout {integer}
    set pmf-sa-query-retry-timeout {integer}
    set okc {disable|enable}
    set mbo {disable|enable}
    set gas-comeback-delay {integer}
    set gas-fragmentation-limit {integer}
    set mbo-cell-data-conn-pref {excluded|prefer-not|...}
    set voice-enterprise {disable|enable}
    set neighbor-report-dual-band {disable|enable}
    set fast-bss-transition {disable|enable}
    set ft-mobility-domain {integer}
    set ft-r0-key-lifetime {integer}
    set ft-over-ds {disable|enable}
    set sae-groups {option1}, {option2}, ...
    set owe-groups {option1}, {option2}, ...
    set owe-transition {disable|enable}
    set owe-transition-ssid {string}
    set additional-akms {option1}, {option2}, ...
    set eapol-key-retries {disable|enable}
```

```
set tkip-counter-measure [enable|disable]
set external-web {var-string}
set external-web-format [auto-detect|no-query-string|...]
set external-logout {string}
set mac-username-delimiter [hyphen|single-hyphen|...]
set mac-password-delimiter [hyphen|single-hyphen|...]
set mac-calling-station-delimiter [hyphen|single-hyphen|...]
set mac-called-station-delimiter [hyphen|single-hyphen|...]
set mac-case [uppercase|lowercase]
set mac-auth-bypass [enable|disable]
set radius-mac-auth [enable|disable]
set radius-mac-auth-server {string}
set radius-mac-auth-usergroups <name1>, <name2>, ...
set auth [psk|radius|...]
set encrypt [TKIP|AES|...]
set keyindex {integer}
set key {password}
set passphrase {password}
set sae-password {password}
set radius-server {string}
set local-standalone [enable|disable]
set local-standalone-nat [enable|disable]
set ip {ipv4-classnet-host}
set dhcp-lease-time {integer}
set local-standalone-dns [enable|disable]
set local-standalone-dns-ip {ipv4-address}
set local-bridging [enable|disable]
set local-lan [allow|deny]
set local-authentication [enable|disable]
set usergroup <name1>, <name2>, ...
set portal-message-override-group {string}
config portal-message-overrides
    Description: Individual message overrides.
    set auth-disclaimer-page {string}
    set auth-reject-page {string}
    set auth-login-page {string}
    set auth-login-failed-page {string}
end
set portal-type [auth|auth+disclaimer|...]
set selected-usergroups <name1>, <name2>, ...
set security-exempt-list {string}
set security-redirect-url {var-string}
set intra-vap-privacy [enable|disable]
set schedule <name1>, <name2>, ...
set ldpc [disable|rx|...]
set high-efficiency [enable|disable]
set target-wake-time [enable|disable]
set port-macauth [disable|radius|...]
set port-macauth-timeout {integer}
set port-macauth-reauth-timeout {integer}
set bss-color-partial [enable|disable]
set mpsk-profile {string}
set split-tunneling [enable|disable]
set nac [enable|disable]
set nac-profile {string}
set vlanid {integer}
set vlan-auto [enable|disable]
```

```
set dynamic-vlan [enable|disable]
set captive-portal-ac-name {string}
set captive-portal-auth-timeout {integer}
set multicast-rate [0|6000|...]
set multicast-enhance [enable|disable]
set igmp-snooping [enable|disable]
set dhcp-address-enforcement [enable|disable]
set broadcast-suppression {option1}, {option2}, ...
set ipv6-rules {option1}, {option2}, ...
set me-disable-thresh {integer}
set mu-mimo [enable|disable]
set probe-resp-suppression [enable|disable]
set probe-resp-threshold {string}
set radio-sensitivity [enable|disable]
set quarantine [enable|disable]
set radio-5g-threshold {string}
set radio-2g-threshold {string}
set wlan-pooling [wtp-group|round-robin|...]
config wlan-pool
    Description: VLAN pool.
    edit <id>
        set wtp-group {string}
    next
end
set dhcp-option43-insertion [enable|disable]
set dhcp-option82-insertion [enable|disable]
set dhcp-option82-circuit-id-insertion [style-1|style-2|...]
set dhcp-option82-remote-id-insertion [style-1|disable]
set ptk-rekey [enable|disable]
set ptk-rekey-intv {integer}
set gtk-rekey [enable|disable]
set gtk-rekey-intv {integer}
set eap-reauth [enable|disable]
set eap-reauth-intv {integer}
set qos-profile {string}
set hotspot20-profile {string}
set access-control-list {string}
set primary-wag-profile {string}
set secondary-wag-profile {string}
set tunnel-echo-interval {integer}
set tunnel-fallback-interval {integer}
set rates-11a {option1}, {option2}, ...
set rates-11bg {option1}, {option2}, ...
set rates-11n-ss12 {option1}, {option2}, ...
set rates-11n-ss34 {option1}, {option2}, ...
set rates-11ac-ss12 {option1}, {option2}, ...
set rates-11ac-ss34 {option1}, {option2}, ...
set utm-profile {string}
set utm-status [enable|disable]
set utm-log [enable|disable]
set ips-sensor {string}
set application-list {string}
set antivirus-profile {string}
set webfilter-profile {string}
set scan-botnet-connections [disable|monitor|...]
set address-group {string}
set mac-filter [enable|disable]
```

```

set mac-filter-policy-other [allow|deny]
config mac-filter-list
    Description: Create a list of MAC addresses for MAC address filtering.
    edit <id>
        set mac {mac-address}
        set mac-filter-policy [allow|deny]
    next
end
set sticky-client-remove [enable|disable]
set sticky-client-threshold-5g {string}
set sticky-client-threshold-2g {string}
set bstm-rssi-disassoc-timer {integer}
set bstm-load-balancing-disassoc-timer {integer}
set bstm-disassociation-imminent [enable|disable]
next
end

```

config wireless-controller vap

Parameter	Description	Type	Size	Default
fast-roaming	Enable/disable fast-roaming, or pre-authentication, where supported by clients .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable fast-roaming, or pre-authentication.		
	<i>disable</i>	Disable fast-roaming, or pre-authentication.		
external-fast-roaming	Enable/disable fast roaming or pre-authentication with external APs not managed by the FortiGate .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable fast roaming or pre-authentication with external APs.		
	<i>disable</i>	Disable fast roaming or pre-authentication with external APs.		
mesh-backhaul	Enable/disable using this VAP as a WiFi mesh backhaul . This entry is only available when security is set to a WPA type or open.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable mesh backhaul.		
	<i>disable</i>	Disable mesh backhaul.		
atf-weight	Airtime weight in percentage .	integer	Minimum value: 0 Maximum value: 100	20

Parameter	Description	Type	Size	Default																						
max-clients	Maximum number of clients that can connect simultaneously to the VAP .	integer	Minimum value: 0 Maximum value: 4294967295	0																						
max-clients-ap	Maximum number of clients that can connect simultaneously to the VAP per AP radio .	integer	Minimum value: 0 Maximum value: 4294967295	0																						
ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string	Maximum length: 32	fortinet																						
broadcast-ssid	Enable/disable broadcasting the SSID .	option	-	enable																						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable broadcasting the SSID.</td></tr> <tr> <td><i>disable</i></td><td>Disable broadcasting the SSID.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable broadcasting the SSID.	<i>disable</i>	Disable broadcasting the SSID.																
Option	Description																									
<i>enable</i>	Enable broadcasting the SSID.																									
<i>disable</i>	Disable broadcasting the SSID.																									
security	Security mode for the wireless interface .	option	-	wpa2-only-personal																						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>open</i></td><td>Open.</td></tr> <tr> <td><i>captive-portal</i></td><td>Captive portal.</td></tr> <tr> <td><i>wep64</i></td><td>WEP 64-bit.</td></tr> <tr> <td><i>wep128</i></td><td>WEP 128-bit.</td></tr> <tr> <td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr> <tr> <td><i>wpa-personal+captive-portal</i></td><td>WPA/WPA2 personal with captive portal.</td></tr> <tr> <td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr> <tr> <td><i>wpa-only-personal</i></td><td>WPA personal.</td></tr> <tr> <td><i>wpa-only-personal+captive-portal</i></td><td>WPA personal with captive portal.</td></tr> <tr> <td><i>wpa-only-enterprise</i></td><td>WPA enterprise.</td></tr> </tbody> </table>					Option	Description	<i>open</i>	Open.	<i>captive-portal</i>	Captive portal.	<i>wep64</i>	WEP 64-bit.	<i>wep128</i>	WEP 128-bit.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.	<i>wpa-only-personal</i>	WPA personal.	<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.	<i>wpa-only-enterprise</i>	WPA enterprise.
Option	Description																									
<i>open</i>	Open.																									
<i>captive-portal</i>	Captive portal.																									
<i>wep64</i>	WEP 64-bit.																									
<i>wep128</i>	WEP 128-bit.																									
<i>wpa-personal</i>	WPA/WPA2 personal.																									
<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.																									
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.																									
<i>wpa-only-personal</i>	WPA personal.																									
<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.																									
<i>wpa-only-enterprise</i>	WPA enterprise.																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wpa2-only-personal</i>	WPA2 personal.		
	<i>wpa2-only-personal+captive-portal</i>	WPA2 personal with captive portal.		
	<i>wpa2-only-enterprise</i>	WPA2 enterprise.		
	<i>wpa3-enterprise</i>	WPA3 enterprise with 192-bit encryption and PMF mandatory.		
	<i>wpa3-only-enterprise</i>	WPA3 enterprise with PMF mandatory.		
	<i>wpa3-enterprise-transition</i>	WPA3 enterprise with PMF optional.		
	<i>wpa3-sae</i>	WPA3 SAE.		
	<i>wpa3-sae-transition</i>	WPA3 SAE transition.		
	<i>owe</i>	Opportunistic wireless encryption.		
	<i>osen</i>	OSEN.		
pmf	Protected Management Frames .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable PMF completely.		
	<i>enable</i>	Enable PMF but deny clients without PMF.		
	<i>optional</i>	Enable PMF and allow clients without PMF.		
pmf-assoc-comeback-timeout	Protected Management Frames .	integer	Minimum value: 1 Maximum value: 20	1
pmf-sa-query-retry-timeout	Protected Management Frames .	integer	Minimum value: 1 Maximum value: 5	2
okc	Enable/disable Opportunistic Key Caching .	option	-	enable
	Option	Description		
	<i>disable</i>	Disable Opportunistic Key Caching (OKC).		
	<i>enable</i>	Enable Opportunistic Key Caching (OKC).		

Parameter	Description	Type	Size	Default
mbo	Enable/disable Multiband Operation .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Multiband Operation (MBO).		
	<i>enable</i>	Enable Multiband Operation (MBO).		
gas-comeback-delay	GAS comeback delay .	integer	Minimum value: 100 Maximum value: 10000	500
gas-fragmentation-limit	GAS fragmentation limit .	integer	Minimum value: 512 Maximum value: 4096	1024
mbo-cell-data-conn-pref	MBO cell data connection preference .	option	-	prefer-not
	Option	Description		
	<i>excluded</i>	Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.		
	<i>prefer-not</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.		
	<i>prefer-use</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.		
voice-enterprise	Enable/disable 802.11k and 802.11v assisted Voice-Enterprise roaming .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.		
	<i>enable</i>	Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.		
neighbor-report-dual-band	Enable/disable dual-band neighbor report .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable dual-band neighbor report.		
	<i>enable</i>	Enable dual-band neighbor report.		
fast-bss-transition	Enable/disable 802.11r Fast BSS Transition .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable 802.11r Fast BSS Transition (FT).		
	<i>enable</i>	Enable 802.11r Fast BSS Transition (FT).		
ft-mobility-domain	Mobility domain identifier in FT .	integer	Minimum value: 1 Maximum value: 65535	1000
ft-r0-key-lifetime	Lifetime of the PMK-R0 key in FT, 1-65535 minutes.	integer	Minimum value: 1 Maximum value: 65535	480
ft-over-ds	Enable/disable FT over the Distribution System (DS).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable FT over the Distribution System (DS).		
	<i>enable</i>	Enable FT over the Distribution System (DS).		
sae-groups	SAE-Groups.	option	-	
	Option	Description		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
owe-groups	OWE-Groups.	option	-	
	Option	Description		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
owe-transition	Enable/disable OWE transition mode support.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable OWE transition mode support.		
	<i>enable</i>	Enable OWE transition mode support.		

Parameter	Description	Type	Size	Default
owe-transition-ssid	OWE transition mode peer SSID.	string	Maximum length: 32	
additional-akms	Additional AKMs.	option	-	
Option		Description		
		<i>akm6</i> Use AKM suite employing PSK_SHA256.		
eapol-key-retries	Enable/disable retransmission of EAPOL-Key frames .	option	-	enable
Option		Description		
		<i>disable</i> Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).		
		<i>enable</i> Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).		
tkip-counter-measure	Enable/disable TKIP counter measure.	option	-	enable
Option		Description		
		<i>enable</i> Enable TKIP counter measure.		
		<i>disable</i> Disable TKIP counter measure.		
external-web	URL of external authentication web server.	var-string	Maximum length: 1023	
external-web-format	URL query parameter detection .	option	-	auto-detect
Option		Description		
		<i>auto-detect</i> Automatically detect if "external-web" URL has any query parameter.		
		<i>no-query-string</i> "external-web" URL does not have any query parameter.		
		<i>partial-query-string</i> "external-web" URL has some query parameters.		
external-logout	URL of external authentication logout server.	string	Maximum length: 127	
mac-username-delimiter	MAC authentication username delimiter .	option	-	hyphen

Parameter	Description	Type	Size	Default
	Option	Description		
		<i>hyphen</i> Use hyphen as delimiter for MAC auth username.		
		<i>single-hyphen</i> Use single hyphen as delimiter for MAC auth username.		
		<i>colon</i> Use colon as delimiter for MAC auth username.		
		<i>none</i> No delimiter for MAC auth username.		
mac-password-delimiter	MAC authentication password delimiter .	option	-	hyphen
	Option	Description		
		<i>hyphen</i> Use hyphen as delimiter for MAC auth password.		
		<i>single-hyphen</i> Use single hyphen as delimiter for MAC auth password.		
		<i>colon</i> Use colon as delimiter for MAC auth password.		
		<i>none</i> No delimiter for MAC auth password.		
mac-calling-station-delimiter	MAC calling station delimiter .	option	-	hyphen
	Option	Description		
		<i>hyphen</i> Use hyphen as delimiter for calling station.		
		<i>single-hyphen</i> Use single hyphen as delimiter for calling station.		
		<i>colon</i> Use colon as delimiter for calling station.		
		<i>none</i> No delimiter for calling station.		
mac-called-station-delimiter	MAC called station delimiter .	option	-	hyphen
	Option	Description		
		<i>hyphen</i> Use hyphen as delimiter for called station.		
		<i>single-hyphen</i> Use single hyphen as delimiter for called station.		
		<i>colon</i> Use colon as delimiter for called station.		
		<i>none</i> No delimiter for called station.		
mac-case	MAC case .	option	-	uppercase
	Option	Description		
		<i>uppercase</i> Use uppercase MAC.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>lowercase</i>	Use lowercase MAC.		
mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable MAC authentication bypass.		
	<i>disable</i>	Disable MAC authentication bypass.		
radius-mac-auth	Enable/disable RADIUS-based MAC authentication of clients .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable RADIUS-based MAC authentication.		
	<i>disable</i>	Disable RADIUS-based MAC authentication.		
radius-mac-auth-server	RADIUS-based MAC authentication server.	string	Maximum length: 35	
radius-mac-auth-usergroups <name>	Selective user groups that are permitted for RADIUS mac authentication. User group name.	string	Maximum length: 79	
auth	Authentication protocol.	option	-	psk
	Option	Description		
	<i>psk</i>	Use a single Pre-share Key (PSK) to authenticate all users.		
	<i>radius</i>	Use a RADIUS server to authenticate clients.		
	<i>usergroup</i>	Use a firewall usergroup to authenticate clients.		
encrypt	Encryption protocol to use (only available when security is set to a WPA type).	option	-	AES
	Option	Description		
	<i>TKIP</i>	Use TKIP encryption.		
	<i>AES</i>	Use AES encryption.		
	<i>TKIP-AES</i>	Use TKIP and AES encryption.		
keyindex	WEP key index .	integer	Minimum value: 1 Maximum value: 4	1

Parameter	Description	Type	Size	Default						
key	WEP Key.	password	Not Specified							
passphrase	WPA pre-shared key (PSK) to be used to authenticate WiFi users.	password	Not Specified							
sae-password	WPA3 SAE password to be used to authenticate WiFi users.	password	Not Specified							
radius-server	RADIUS server to be used to authenticate WiFi users.	string	Maximum length: 35							
local-standalone	Enable/disable AP local standalone .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable AP local standalone.</td></tr> <tr> <td><i>disable</i></td><td>Disable AP local standalone.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable AP local standalone.	<i>disable</i>	Disable AP local standalone.
Option	Description									
<i>enable</i>	Enable AP local standalone.									
<i>disable</i>	Disable AP local standalone.									
local-standalone-nat	Enable/disable AP local standalone NAT mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable AP local standalone NAT mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable AP local standalone NAT mode.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable AP local standalone NAT mode.	<i>disable</i>	Disable AP local standalone NAT mode.
Option	Description									
<i>enable</i>	Enable AP local standalone NAT mode.									
<i>disable</i>	Disable AP local standalone NAT mode.									
ip	IP address and subnet mask for the local standalone NAT subnet.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0						
dhcp-lease-time	DHCP lease time in seconds for NAT IP address.	integer	Minimum value: 300 Maximum value: 8640000	2400						
local-standalone-dns	Enable/disable AP local standalone DNS.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable AP local standalone DNS.</td></tr> <tr> <td><i>disable</i></td><td>Disable AP local standalone DNS.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable AP local standalone DNS.	<i>disable</i>	Disable AP local standalone DNS.
Option	Description									
<i>enable</i>	Enable AP local standalone DNS.									
<i>disable</i>	Disable AP local standalone DNS.									
local-standalone-dns-ip	IPv4 addresses for the local standalone DNS.	ipv4-address	Not Specified							
local-bridging	Enable/disable bridging of wireless and Ethernet interfaces on the FortiAP .	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable AP local VAP to Ethernet bridging.		
	<i>disable</i>	Disable AP local VAP to Ethernet bridging.		
local-lan	Allow/deny traffic destined for a Class A, B, or C private IP address .	option	-	allow
	Option	Description		
	<i>allow</i>	Allow traffic destined for a Class A, B, or C private IP address.		
	<i>deny</i>	Deny traffic destined for a Class A, B, or C private IP address.		
local-authentication	Enable/disable AP local authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable AP local authentication.		
	<i>disable</i>	Disable AP local authentication.		
usergroup <name>	Firewall user group to be used to authenticate WiFi users. User group name.	string	Maximum length: 79	
portal-message-override-group	Replacement message group for this VAP (only available when security is set to a captive portal type).	string	Maximum length: 35	
portal-type	Captive portal functionality. Configure how the captive portal authenticates users and whether it includes a disclaimer.	option	-	auth
	Option	Description		
	<i>auth</i>	Portal for authentication.		
	<i>auth+disclaimer</i>	Portal for authentication and disclaimer.		
	<i>disclaimer</i>	Portal for disclaimer.		
	<i>email-collect</i>	Portal for email collection.		
	<i>cmcc</i>	Portal for CMCC.		
	<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.		
	<i>auth-mac</i>	Portal for authentication and MAC authentication.		
	<i>external-auth</i>	Portal for external portal authentication.		
	<i>external-macauth</i>	Portal for external portal MAC authentication.		

Parameter	Description	Type	Size	Default										
selected-usergroups <name>	Selective user groups that are permitted to authenticate. User group name.	string	Maximum length: 79											
security-exempt-list	Optional security exempt list for captive portal authentication.	string	Maximum length: 35											
security-redirect-url	Optional URL for redirecting users after they pass captive portal authentication.	var-string	Maximum length: 1023											
intra-vap-privacy	Enable/disable blocking communication between clients on the same SSID .	option	-	disable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable intra-SSID privacy.</td></tr> <tr> <td>disable</td><td>Disable intra-SSID privacy.</td></tr> </tbody> </table>					Option	Description	enable	Enable intra-SSID privacy.	disable	Disable intra-SSID privacy.				
Option	Description													
enable	Enable intra-SSID privacy.													
disable	Disable intra-SSID privacy.													
schedule <name>	Firewall schedules for enabling this VAP on the FortiAP. This VAP will be enabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35											
ldpc	VAP low-density parity-check (LDPC) coding configuration.	option	-	rxtx										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>disable</td><td>Disable LDPC.</td></tr> <tr> <td>rx</td><td>Enable LDPC when receiving traffic.</td></tr> <tr> <td>tx</td><td>Enable LDPC when transmitting traffic.</td></tr> <tr> <td>rxtx</td><td>Enable LDPC when both receiving and transmitting traffic.</td></tr> </tbody> </table>					Option	Description	disable	Disable LDPC.	rx	Enable LDPC when receiving traffic.	tx	Enable LDPC when transmitting traffic.	rxtx	Enable LDPC when both receiving and transmitting traffic.
Option	Description													
disable	Disable LDPC.													
rx	Enable LDPC when receiving traffic.													
tx	Enable LDPC when transmitting traffic.													
rxtx	Enable LDPC when both receiving and transmitting traffic.													
high-efficiency	Enable/disable 802.11ax high efficiency .	option	-	enable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable 802.11ax high efficiency.</td></tr> <tr> <td>disable</td><td>Disable 802.11ax high efficiency.</td></tr> </tbody> </table>					Option	Description	enable	Enable 802.11ax high efficiency.	disable	Disable 802.11ax high efficiency.				
Option	Description													
enable	Enable 802.11ax high efficiency.													
disable	Disable 802.11ax high efficiency.													
target-wake-time	Enable/disable 802.11ax target wake time .	option	-	enable										
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>enable</td><td>Enable 802.11ax target wake time.</td></tr> <tr> <td>disable</td><td>Disable 802.11ax target wake time.</td></tr> </tbody> </table>					Option	Description	enable	Enable 802.11ax target wake time.	disable	Disable 802.11ax target wake time.				
Option	Description													
enable	Enable 802.11ax target wake time.													
disable	Disable 802.11ax target wake time.													

Parameter	Description	Type	Size	Default								
port-macauth	Enable/disable LAN port MAC authentication .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable LAN port MAC authentication.</td></tr> <tr> <td><i>radius</i></td><td>Enable LAN port RADIUS-based MAC authentication.</td></tr> <tr> <td><i>address-group</i></td><td>Enable LAN port address-group based MAC authentication.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable LAN port MAC authentication.	<i>radius</i>	Enable LAN port RADIUS-based MAC authentication.	<i>address-group</i>	Enable LAN port address-group based MAC authentication.			
Option	Description											
<i>disable</i>	Disable LAN port MAC authentication.											
<i>radius</i>	Enable LAN port RADIUS-based MAC authentication.											
<i>address-group</i>	Enable LAN port address-group based MAC authentication.											
port-macauth-timeout	LAN port MAC authentication idle timeout value .	integer	Minimum value: 60 Maximum value: 65535	600								
port-macauth-reauth-timeout	LAN port MAC authentication re-authentication timeout value .	integer	Minimum value: 120 Maximum value: 65535	7200								
bss-color-partial	Enable/disable 802.11ax partial BSS color .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable 802.11ax partial BSS color.</td></tr> <tr> <td><i>disable</i></td><td>Disable 802.11ax partial BSS color.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable 802.11ax partial BSS color.	<i>disable</i>	Disable 802.11ax partial BSS color.					
Option	Description											
<i>enable</i>	Enable 802.11ax partial BSS color.											
<i>disable</i>	Disable 802.11ax partial BSS color.											
mpsk-profile	MPSK profile name.	string	Maximum length: 35									
split-tunneling	Enable/disable split tunneling .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable split tunneling.</td></tr> <tr> <td><i>disable</i></td><td>Disable split tunneling.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable split tunneling.	<i>disable</i>	Disable split tunneling.					
Option	Description											
<i>enable</i>	Enable split tunneling.											
<i>disable</i>	Disable split tunneling.											
nac	Enable/disable network access control.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable network access control.</td></tr> <tr> <td><i>disable</i></td><td>Disable network access control.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable network access control.	<i>disable</i>	Disable network access control.					
Option	Description											
<i>enable</i>	Enable network access control.											
<i>disable</i>	Disable network access control.											
nac-profile	NAC profile name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default
vlanid	Optional VLAN ID.	integer	Minimum value: 0 Maximum value: 4094	0
vlan-auto	Enable/disable automatic management of SSID VLAN interface.	option	-	disable
Option		Description		
		<i>enable</i> Enable automatic management of SSID VLAN interface.		
		<i>disable</i> Disable automatic management of SSID VLAN interface.		
dynamic-vlan	Enable/disable dynamic VLAN assignment.	option	-	disable
Option		Description		
		<i>enable</i> Enable dynamic VLAN assignment.		
		<i>disable</i> Disable dynamic VLAN assignment.		
captive-portal-ac-name	Local-bridging captive portal ac-name.	string	Maximum length: 35	
captive-portal-auth-timeout	Hard timeout - AP will always clear the session after timeout regardless of traffic .	integer	Minimum value: 0 Maximum value: 864000	0
multicast-rate	Multicast rate .	option	-	0
Option		Description		
		<i>0</i> Use the default multicast rate.		
		<i>6000</i> 6 Mbps.		
		<i>12000</i> 12 Mbps.		
		<i>24000</i> 24 Mbps.		
multicast-enhance	Enable/disable converting multicast to unicast to improve performance .	option	-	disable
Option		Description		
		<i>enable</i> Enable multicast enhancement.		
		<i>disable</i> Disable multicast enhancement.		
igmp-snooping	Enable/disable IGMP snooping.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable IGMP snooping.		
	<i>disable</i>	Disable IGMP snooping.		
dhcp-address-enforcement	Enable/disable DHCP address enforcement .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.		
	<i>disable</i>	Disable DHCP enforcement, clients can access the network without DHCP process.		
broadcast-suppression	Optional suppression of broadcast messages. For example, you can keep DHCP messages, ARP broadcasts, and so on off of the wireless network.	option	-	dhcp-up dhcp-ucast arp-known
	Option	Description		
	<i>dhcp-up</i>	Suppress broadcast uplink DHCP messages.		
	<i>dhcp-down</i>	Suppress broadcast downlink DHCP messages.		
	<i>dhcp-starvation</i>	Suppress broadcast DHCP starvation req messages.		
	<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.		
	<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.		
	<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.		
	<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.		
	<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.		
	<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.		
	<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.		
	<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.		
	<i>ipv6</i>	Suppress IPv6 packets.		
	<i>all-other-mc</i>	Suppress all other multicast messages.		
	<i>all-other-bc</i>	Suppress all other broadcast messages.		

Parameter	Description	Type	Size	Default																				
ipv6-rules	Optional rules of IPv6 packets. For example, you can keep RA, RS and so on off of the wireless network.	option	-	drop-icmp6ra drop-icmp6rs drop-llmnr6 drop-icmp6mld2 drop-dhcp6s drop-dhcp6c ndp-proxy drop-ns-dad																				
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>drop-icmp6ra</i></td><td>Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.</td></tr> <tr> <td><i>drop-icmp6rs</i></td><td>Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.</td></tr> <tr> <td><i>drop-llmnr6</i></td><td>Drop Link-Local Multicast Name Resolution (LLMNR) packets</td></tr> <tr> <td><i>drop-icmp6mld2</i></td><td>Drop ICMP6 Multicast Listener Report V2 (MLD2) packets</td></tr> <tr> <td><i>drop-dhcp6s</i></td><td>Drop DHCP6 server generated packets that originate from wireless clients.</td></tr> <tr> <td><i>drop-dhcp6c</i></td><td>Drop DHCP6 client generated packets to be sent to wireless clients.</td></tr> <tr> <td><i>ndp-proxy</i></td><td>Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.</td></tr> <tr> <td><i>drop-ns-dad</i></td><td>Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.</td></tr> <tr> <td><i>drop-ns-nondad</i></td><td>Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.</td></tr> </tbody> </table>					Option	Description	<i>drop-icmp6ra</i>	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.	<i>drop-icmp6rs</i>	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.	<i>drop-llmnr6</i>	Drop Link-Local Multicast Name Resolution (LLMNR) packets	<i>drop-icmp6mld2</i>	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets	<i>drop-dhcp6s</i>	Drop DHCP6 server generated packets that originate from wireless clients.	<i>drop-dhcp6c</i>	Drop DHCP6 client generated packets to be sent to wireless clients.	<i>ndp-proxy</i>	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.	<i>drop-ns-dad</i>	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.	<i>drop-ns-nondad</i>	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.
Option	Description																							
<i>drop-icmp6ra</i>	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.																							
<i>drop-icmp6rs</i>	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.																							
<i>drop-llmnr6</i>	Drop Link-Local Multicast Name Resolution (LLMNR) packets																							
<i>drop-icmp6mld2</i>	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets																							
<i>drop-dhcp6s</i>	Drop DHCP6 server generated packets that originate from wireless clients.																							
<i>drop-dhcp6c</i>	Drop DHCP6 client generated packets to be sent to wireless clients.																							
<i>ndp-proxy</i>	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.																							
<i>drop-ns-dad</i>	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.																							
<i>drop-ns-nondad</i>	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.																							
me-disable-thresh	Disable multicast enhancement when this many clients are receiving multicast traffic.	integer	Minimum value: 2 Maximum value: 256	32																				
mu-mimo	Enable/disable Multi-user MIMO .	option	-	enable																				
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable Multi-user MIMO.</td></tr> <tr> <td><i>disable</i></td><td>Disable Multi-user MIMO.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable Multi-user MIMO.	<i>disable</i>	Disable Multi-user MIMO.														
Option	Description																							
<i>enable</i>	Enable Multi-user MIMO.																							
<i>disable</i>	Disable Multi-user MIMO.																							
probe-resp-suppression	Enable/disable probe response suppression .	option	-	disable																				
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable probe response suppression.</td></tr> <tr> <td><i>disable</i></td><td>Disable probe response suppression.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable probe response suppression.	<i>disable</i>	Disable probe response suppression.														
Option	Description																							
<i>enable</i>	Enable probe response suppression.																							
<i>disable</i>	Disable probe response suppression.																							

Parameter	Description	Type	Size	Default
probe-resp-threshold	Minimum signal level/threshold in dBm required for the AP response to probe requests .	string	Maximum length: 7	-80
radio-sensitivity	Enable/disable software radio sensitivity .	option	-	disable
Option		Description		
<i>enable</i>		Enable software radio sensitivity.		
<i>disable</i>		Disable software radio sensitivity.		
quarantine	Enable/disable station quarantine .	option	-	enable
Option		Description		
<i>enable</i>		Enable station quarantine.		
<i>disable</i>		Disable station quarantine.		
radio-5g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 5G band.	string	Maximum length: 7	-76
radio-2g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 2.4G band .	string	Maximum length: 7	-79
vlan-pooling	Enable/disable VLAN pooling, to allow grouping of multiple wireless controller VLANs into VLAN pools . When set to wtp-group, VLAN pooling occurs with VLAN assignment by wtp-group.	option	-	disable
Option		Description		
<i>wtp-group</i>		Enable VLAN pooling with VLAN assignment by wtp-group.		
<i>round-robin</i>		Enable VLAN pooling with round-robin VLAN assignment.		
<i>hash</i>		Enable VLAN pooling with hash-based VLAN assignment.		
<i>disable</i>		Disable VLAN pooling.		
dhcp-option43-insertion	Enable/disable insertion of DHCP option 43 .	option	-	enable
Option		Description		
<i>enable</i>		Enable insertion of DHCP option 43.		
<i>disable</i>		Disable insertion of DHCP option 43.		

Parameter	Description	Type	Size	Default
dhcp-option82-insertion	Enable/disable DHCP option 82 insert .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DHCP option 82 insert.		
	<i>disable</i>	Disable DHCP option 82 insert.		
dhcp-option82-circuit-id-insertion	Enable/disable DHCP option 82 circuit-id insert .	option	-	disable
	Option	Description		
	<i>style-1</i>	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:wifi;s".		
	<i>style-2</i>	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".		
	<i>style-3</i>	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example, "WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".		
	<i>disable</i>	Disable DHCP option 82 circuit-id insert.		
dhcp-option82-remote-id-insertion	Enable/disable DHCP option 82 remote-id insert .	option	-	disable
	Option	Description		
	<i>style-1</i>	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.		
	<i>disable</i>	Disable DHCP option 82 remote-id insert.		
ptk-rekey	Enable/disable PTK rekey for WPA-Enterprise security.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.		
	<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.		
ptk-rekey-intv	PTK rekey interval .	integer	Minimum value: 1800 Maximum value: 864000	86400

Parameter	Description	Type	Size	Default
gtk-rekey	Enable/disable GTK rekey for WPA security.	option	-	disable
	Option	Description		
	enable	Enable GTK rekey for WPA security.		
	disable	Disable GTK rekey for WPA security.		
gtk-rekey-intv	GTK rekey interval .	integer	Minimum value: 1800 Maximum value: 864000	86400
eap-reauth	Enable/disable EAP re-authentication for WPA-Enterprise security.	option	-	disable
	Option	Description		
	enable	Enable EAP re-authentication for WPA-Enterprise security.		
	disable	Disable EAP re-authentication for WPA-Enterprise security.		
eap-reauth-intv	EAP re-authentication interval .	integer	Minimum value: 1800 Maximum value: 864000	86400
qos-profile	Quality of service profile name.	string	Maximum length: 35	
hotspot20-profile	Hotspot 2.0 profile name.	string	Maximum length: 35	
access-control-list	access-control-list profile name.	string	Maximum length: 35	
primary-wag-profile	Primary wireless access gateway profile name.	string	Maximum length: 35	
secondary-wag-profile	Secondary wireless access gateway profile name.	string	Maximum length: 35	
tunnel-echo-interval	The time interval to send echo to both primary and secondary tunnel peers .	integer	Minimum value: 1 Maximum value: 65535	300
tunnel-fallback-interval	The time interval for secondary tunnel to fall back to primary tunnel .	integer	Minimum value: 0 Maximum value: 65535	7200
rates-11a	Allowed data rates for 802.11a.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	1	1 Mbps supported rate.		
	1-basic	1 Mbps BSS basic rate.		
	2	2 Mbps supported rate.		
	2-basic	2 Mbps BSS basic rate.		
	5.5	5.5 Mbps supported rate.		
	5.5-basic	5.5 Mbps BSS basic rate.		
	11	11 Mbps supported rate.		
	11-basic	11 Mbps BSS basic rate.		
	6	6 Mbps supported rate.		
	6-basic	6 Mbps BSS basic rate.		
	9	9 Mbps supported rate.		
	9-basic	9 Mbps BSS basic rate.		
	12	12 Mbps supported rate.		
	12-basic	12 Mbps BSS basic rate.		
	18	18 Mbps supported rate.		
	18-basic	18 Mbps BSS basic rate.		
	24	24 Mbps supported rate.		
	24-basic	24 Mbps BSS basic rate.		
	36	36 Mbps supported rate.		
	36-basic	36 Mbps BSS basic rate.		
	48	48 Mbps supported rate.		
	48-basic	48 Mbps BSS basic rate.		
	54	54 Mbps supported rate.		
	54-basic	54 Mbps BSS basic rate.		
rates-11bg	Allowed data rates for 802.11b/g.	option	-	
	Option	Description		
	1	1 Mbps supported rate.		
	1-basic	1 Mbps BSS basic rate.		

Parameter	Description	Type	Size	Default
	Option	Description		
	2	2 Mbps supported rate.		
	2-basic	2 Mbps BSS basic rate.		
	5.5	5.5 Mbps supported rate.		
	5.5-basic	5.5 Mbps BSS basic rate.		
	11	11 Mbps supported rate.		
	11-basic	11 Mbps BSS basic rate.		
	6	6 Mbps supported rate.		
	6-basic	6 Mbps BSS basic rate.		
	9	9 Mbps supported rate.		
	9-basic	9 Mbps BSS basic rate.		
	12	12 Mbps supported rate.		
	12-basic	12 Mbps BSS basic rate.		
	18	18 Mbps supported rate.		
	18-basic	18 Mbps BSS basic rate.		
	24	24 Mbps supported rate.		
	24-basic	24 Mbps BSS basic rate.		
	36	36 Mbps supported rate.		
	36-basic	36 Mbps BSS basic rate.		
	48	48 Mbps supported rate.		
	48-basic	48 Mbps BSS basic rate.		
	54	54 Mbps supported rate.		
	54-basic	54 Mbps BSS basic rate.		
rates-11n-ss12	Allowed data rates for 802.11n with 1 or 2 spatial streams.	option	-	
	Option	Description		
	mcs0/1	Data rate for MCS index 0 with 1 spatial stream.		
	mcs1/1	Data rate for MCS index 1 with 1 spatial stream.		
	mcs2/1	Data rate for MCS index 2 with 1 spatial stream.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.		
	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.		
	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.		
	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.		
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.		
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.		
	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.		
	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.		
	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.		
	<i>mcs12/2</i>	Data rate for MCS index 12 with 2 spatial streams.		
	<i>mcs13/2</i>	Data rate for MCS index 13 with 2 spatial streams.		
	<i>mcs14/2</i>	Data rate for MCS index 14 with 2 spatial streams.		
	<i>mcs15/2</i>	Data rate for MCS index 15 with 2 spatial streams.		
rates-11n-ss34	Allowed data rates for 802.11n with 3 or 4 spatial streams.	option	-	
	Option	Description		
	<i>mcs16/3</i>	Data rate for MCS index 16 with 3 spatial streams.		
	<i>mcs17/3</i>	Data rate for MCS index 17 with 3 spatial streams.		
	<i>mcs18/3</i>	Data rate for MCS index 18 with 3 spatial streams.		
	<i>mcs19/3</i>	Data rate for MCS index 19 with 3 spatial streams.		
	<i>mcs20/3</i>	Data rate for MCS index 20 with 3 spatial streams.		
	<i>mcs21/3</i>	Data rate for MCS index 21 with 3 spatial streams.		
	<i>mcs22/3</i>	Data rate for MCS index 22 with 3 spatial streams.		
	<i>mcs23/3</i>	Data rate for MCS index 23 with 3 spatial streams.		
	<i>mcs24/4</i>	Data rate for MCS index 24 with 4 spatial streams.		
	<i>mcs25/4</i>	Data rate for MCS index 25 with 4 spatial streams.		
	<i>mcs26/4</i>	Data rate for MCS index 26 with 4 spatial streams.		
	<i>mcs27/4</i>	Data rate for MCS index 27 with 4 spatial streams.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.		
	<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.		
	<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.		
	<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.		
rates-11ac-ss12	Allowed data rates for 802.11ac/ax with 1 or 2 spatial streams.	option	-	
	Option	Description		
	<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.		
	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.		
	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.		
	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.		
	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.		
	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.		
	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.		
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.		
	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.		
	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.		
	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.		
	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.		
	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.		
	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.		
	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.		
	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.		
	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.		
	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.		
	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.		
	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.		
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.		
	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.		
	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.		
rates-11ac-ss34	Allowed data rates for 802.11ac/ax with 3 or 4 spatial streams.	option	-	
	Option	Description		
	<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.		
	<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.		
	<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.		
	<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.		
	<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.		
	<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.		
	<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.		
	<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.		
	<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.		
	<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.		
	<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.		
	<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.		
	<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.		
	<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.		
	<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.		
	<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.		
	<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.		
	<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.		
	<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.		
	<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.		
	<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.		
	<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>mcs 10/4</i>	Data rate for MCS index 10 with 4 spatial streams.		
	<i>mcs 11/4</i>	Data rate for MCS index 11 with 4 spatial streams.		
utm-profile	UTM profile name.	string	Maximum length: 35	
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the VAP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
utm-log	Enable/disable UTM logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable UTM logging.		
	<i>disable</i>	Disable UTM logging.		
ips-sensor	IPS sensor name.	string	Maximum length: 35	
application-list	Application control list name.	string	Maximum length: 35	
antivirus-profile	AntiVirus profile name.	string	Maximum length: 35	
webfilter-profile	WebFilter profile name.	string	Maximum length: 35	
scan-botnet-connections	Block or monitor connections to Botnet servers or disable Botnet scanning.	option	-	monitor
	Option	Description		
	<i>disable</i>	Do not scan connections to botnet servers.		
	<i>monitor</i>	Log connections to botnet servers.		
	<i>block</i>	Block connections to botnet servers.		
address-group	Address group ID.	string	Maximum length: 35	
mac-filter	Enable/disable MAC filtering to block wireless clients by mac address.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable MAC filtering.		
	<i>disable</i>	Disable MAC filtering.		
mac-filter-policy-other	Allow or block clients with MAC addresses that are not in the filter list.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.		
	<i>deny</i>	Block clients with MAC addresses that are not in the filter list.		
sticky-client-remove	Enable/disable sticky client remove to maintain good signal level clients in SSID. .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Sticky Client Remove.		
	<i>disable</i>	Disable Sticky Client Remove.		
sticky-client-threshold-5g	Minimum signal level/threshold in dBm required for the 5G client to be serviced by the AP .	string	Maximum length: 7	-76
sticky-client-threshold-2g	Minimum signal level/threshold in dBm required for the 2G client to be serviced by the AP .	string	Maximum length: 7	-79
bstm-rssi-disassoc-timer	Time interval for client to voluntarily leave AP before forcing a disassociation due to low RSSI .	integer	Minimum value: 1 Maximum value: 2000	200
bstm-load-balancing-disassoc-timer	Time interval for client to voluntarily leave AP before forcing a disassociation due to AP load-balancing .	integer	Minimum value: 1 Maximum value: 30	10
bstm-disassociation-imminent	Enable/disable forcing of disassociation after the BSTM request timer has been reached .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable BSTM Disassociation Imminent.		
	<i>disable</i>	Disable BSTM Disassociation Imminent.		

config portal-message-overrides

Parameter	Description	Type	Size	Default
auth-disclaimer-page	Override auth-disclaimer-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-reject-page	Override auth-reject-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-page	Override auth-login-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-failed-page	Override auth-login-failed-page message with message from portal-message-overrides group.	string	Maximum length: 35	

config vlan-pool

Parameter	Description	Type	Size	Default
wtp-group	WTP group name.	string	Maximum length: 35	

config mac-filter-list

Parameter	Description	Type	Size	Default
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
mac-filter-policy	Deny or allow the client with this MAC address.	option	-	deny
Option		Description		
		allow		Allow the client with this MAC address.
		deny		Block the client with this MAC address.

config wireless-controller timers

Configure CAPWAP timers.

```
config wireless-controller timers
  Description: Configure CAPWAP timers.
  set echo-interval {integer}
  set discovery-interval {integer}
  set client-idle-timeout {integer}
  set rogue-ap-log {integer}
  set fake-ap-log {integer}
  set sta-stats-interval {integer}
  set vap-stats-interval {integer}
```

```

set radio-stats-interval {integer}
set sta-capability-interval {integer}
set sta-locate-timer {integer}
set ipsec-intf-cleanups {integer}
set ble-scan-report-intv {integer}
    set drma-interval {integer}
end

```

config wireless-controller timers

Parameter	Description	Type	Size	Default
echo-interval	Time between echo requests sent by the managed WTP, AP, or FortiAP .	integer	Minimum value: 1 Maximum value: 255	30
discovery-interval	Time between discovery requests .	integer	Minimum value: 2 Maximum value: 180	5
client-idle-timeout	Time after which a client is considered idle and times out .	integer	Minimum value: 20 Maximum value: 3600	300
rogue-ap-log	Time between logging rogue AP messages if periodic rogue AP logging is configured .	integer	Minimum value: 0 Maximum value: 1440	0
fake-ap-log	Time between recording logs about fake APs if periodic fake AP logging is configured .	integer	Minimum value: 1 Maximum value: 1440	1
sta-stats-interval	Time between running client .	integer	Minimum value: 1 Maximum value: 255	1
vap-stats-interval	Time between running Virtual Access Point .	integer	Minimum value: 1 Maximum value: 255	15
radio-stats-interval	Time between running radio reports .	integer	Minimum value: 1 Maximum value: 255	15

Parameter	Description	Type	Size	Default
sta-capability-interval	Time between running station capability reports .	integer	Minimum value: 1 Maximum value: 255	30
sta-locate-timer	Time between running client presence flushes to remove clients that are listed but no longer present .	integer	Minimum value: 0 Maximum value: 86400	1800
ipsec-intf-cleanup	Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected .	integer	Minimum value: 30 Maximum value: 3600	120
ble-scan-report-intv	Time between running Bluetooth Low Energy .	integer	Minimum value: 10 Maximum value: 3600	30
drma-interval	Dynamic radio mode assignment .	integer	Minimum value: 1 Maximum value: 1440	60

config wireless-controller setting

VDOM wireless controller configuration.

```
config wireless-controller setting
  Description: VDOM wireless controller configuration.
  set account-id {string}
  set country [--|AF|...]
  set duplicate-ssid [enable|disable]
  set fapc-compatibility [enable|disable]
  set wfa-compatibility [enable|disable]
  set phishing-ssid-detect [enable|disable]
  set fake-ssid-action {option1}, {option2}, ...
  config offending-ssid
    Description: Configure offending SSID.
    edit <id>
      set ssid-pattern {string}
      set action {option1}, {option2}, ...
    next
  end
  set device-weight {integer}
  set device-holdoff {integer}
  set device-idle {integer}
  set darrp-optimize {integer}
  set darrp-optimize-schedules <name1>, <name2>, ...
end
```

config wireless-controller setting

Parameter	Description	Type	Size	Default
account-id	FortiCloud customer account ID.	string	Maximum length: 63	
country	Country or region in which the FortiGate is located. The country determines the 802.11 bands and channels that are available.	option	-	US
	Option	Description		
	--	NO_COUNTRY_SET		
	AF	AFGHANISTAN		
	AL	ALBANIA		
	DZ	ALGERIA		
	AS	AMERICAN SAMOA		
	AO	ANGOLA		
	AR	ARGENTINA		
	AM	ARMENIA		
	AU	AUSTRALIA		
	AT	AUSTRIA		
	AZ	AZERBAIJAN		
	BS	BAHAMAS		
	BH	BAHRAIN		
	BD	BANGLADESH		
	BB	BARBADOS		
	BY	BELARUS		
	BE	BELGIUM		
	BZ	BELIZE		
	BJ	BENIN		
	BM	BERMUDA		
	BT	BHUTAN		
	BO	BOLIVIA		
	BA	BOSNIA AND HERZEGOVINA		
	BW	BOTSWANA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>BR</i>	BRAZIL		
	<i>BN</i>	BRUNEI DARUSSALAM		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GE</i>	GEORGIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i i="" iq<=""></i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		
	<i>CI</i>	COTE_D_IVOIRE		
	<i>JM</i>	JAMAICA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>JO</i>	JORDAN		
	<i>KZ</i>	KAZAKHSTAN		
	<i>KE</i>	KENYA		
	<i>KR</i>	KOREA REPUBLIC		
	<i>KW</i>	KUWAIT		
	<i>LA</i>	LAOS		
	<i>LV</i>	LATVIA		
	<i>LB</i>	LEBANON		
	<i>LS</i>	LESOTHO		
	<i>LY</i>	LIBYA		
	<i>LI</i>	LIECHTENSTEIN		
	<i>LT</i>	LITHUANIA		
	<i>LU</i>	LUXEMBOURG		
	<i>MO</i>	MACAU SAR		
	<i>MK</i>	MACEDONIA, FYRO		
	<i>MG</i>	MADAGASCAR		
	<i>MW</i>	MALAWI		
	<i>MY</i>	MALAYSIA		
	<i>MV</i>	MALDIVES		
	<i>ML</i>	MALI		
	<i>MT</i>	MALTA		
	<i>MH</i>	MARSHALL ISLANDS		
	<i>MQ</i>	MARTINIQUE		
	<i>MR</i>	MAURITANIA		
	<i>MU</i>	MAURITIUS		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>MC</i>	MONACO		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NA</i>	NAMIBIA		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NO</i>	NORWAY		
	<i>MP</i>	NORTHERN MARIANA ISLANDS		
	<i>OM</i>	OMAN		
	<i>PK</i>	PAKISTAN		
	<i>PW</i>	PALAU		
	<i>PA</i>	PANAMA		
	<i>PG</i>	PAPUA NEW GUINEA		
	<i>PY</i>	PARAGUAY		
	<i>PE</i>	PERU		
	<i>PH</i>	PHILIPPINES		
	<i>PL</i>	POLAND		
	<i>PT</i>	PORTUGAL		
	<i>PR</i>	PUERTO RICO		
	<i>QA</i>	QATAR		
	<i>RE</i>	REUNION		
	<i>RO</i>	ROMANIA		
	<i>RU</i>	RUSSIA		

Parameter	Description	Type	Size	Default
	Option	Description		
<i>RW</i>	RWANDA			
<i>BL</i>	SAINT BARTHELEMY			
<i>KN</i>	SAINT KITTS AND NEVIS			
<i>LC</i>	SAINT LUCIA			
<i>MF</i>	SAINT MARTIN			
<i>PM</i>	SAINT PIERRE AND MIQUELON			
<i>VC</i>	SAINT VINCENT AND GRENADIENS			
<i>SA</i>	SAUDI ARABIA			
<i>SN</i>	SENEGAL			
<i>RS</i>	REPUBLIC OF SERBIA			
<i>ME</i>	MONTENEGRO			
<i>SL</i>	SIERRA LEONE			
<i>SG</i>	SINGAPORE			
<i>SK</i>	SLOVAKIA			
<i>SI</i>	SLOVENIA			
<i>ZA</i>	SOUTH AFRICA			
<i>ES</i>	SPAIN			
<i>LK</i>	SRI LANKA			
<i>SE</i>	SWEDEN			
<i>SR</i>	SURINAME			
<i>CH</i>	SWITZERLAND			
<i>TW</i>	TAIWAN			
<i>TZ</i>	TANZANIA			
<i>TH</i>	THAILAND			
<i>TG</i>	TOGO			
<i>TT</i>	TRINIDAD AND TOBAGO			
<i>TN</i>	TUNISIA			
<i>TR</i>	TURKEY			
<i>TM</i>	TURKMENISTAN			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>AE</i>	UNITED ARAB EMIRATES		
	<i>TC</i>	TURKS AND CAICOS		
	<i>UG</i>	UGANDA		
	<i>UA</i>	UKRAINE		
	<i>GB</i>	UNITED KINGDOM		
	<i>US</i>	UNITED STATES2		
	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)		
	<i>UY</i>	URUGUAY		
	<i>UZ</i>	UZBEKISTAN		
	<i>VU</i>	VANUATU		
	<i>VE</i>	VENEZUELA		
	<i>VN</i>	VIET NAM		
	<i>VI</i>	VIRGIN ISLANDS		
	<i>WF</i>	WALLIS AND FUTUNA		
	<i>YE</i>	YEMEN		
	<i>ZM</i>	ZAMBIA		
	<i>ZW</i>	ZIMBABWE		
	<i>JP</i>	JAPAN14		
	<i>CA</i>	CANADA2		
duplicate-ssid	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.	option	-	disable
	Option	Description		
	<i>enable</i>	Allow VAPs to use the same SSID name in the same VDOM.		
	<i>disable</i>	Do not allow VAPs to use the same SSID name in the same VDOM.		
fapc-compatibility	Enable/disable FAP-C series compatibility.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FAP-C series compatibility.		
	<i>disable</i>	Disable FAP-C series compatibility.		

Parameter	Description	Type	Size	Default
wfa-compatibility	Enable/disable WFA compatibility.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.		
	<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.		
phishing-ssid-detected	Enable/disable phishing SSID detection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable phishing SSID detection.		
	<i>disable</i>	Disable phishing SSID detection.		
fake-ssid-action	Actions taken for detected fake SSID.	option	-	log
	Option	Description		
	<i>log</i>	Write logs for detected fake SSID.		
	<i>suppress</i>	Suppress detected fake SSID.		
device-weight	Upper limit of confidence of device for identification .	integer	Minimum value: 0 Maximum value: 255	1
device-holdoff	Lower limit of creation time of device for identification in minutes .	integer	Minimum value: 0 Maximum value: 60	5
device-idle	Upper limit of idle time of device for identification in minutes .	integer	Minimum value: 0 Maximum value: 14400	1440
darrp-optimize	Time for running Dynamic Automatic Radio Resource Provisioning .	integer	Minimum value: 0 Maximum value: 86400	86400

Parameter	Description	Type	Size	Default
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35	

config offending-ssid

Parameter	Description	Type	Size	Default
ssid-pattern	Define offending SSID pattern (case insensitive), eg: word, word*, *word, wo*rd.	string	Maximum length: 33	
action	Actions taken for detected offending SSID.	option	-	log
Option		Description		
		<i>log</i> Generate logs for detected offending SSID.		
		<i>suppress</i> Suppress detected offending SSID.		

config wireless-controller log

Configure wireless controller event log filters.

```
config wireless-controller log
  Description: Configure wireless controller event log filters.
  set status [enable|disable]
  set addrgrp-log [emergency|alert|...]
  set ble-log [emergency|alert|...]
  set clb-log [emergency|alert|...]
  set dhcp-starv-log [emergency|alert|...]
  set led-sched-log [emergency|alert|...]
  set radio-event-log [emergency|alert|...]
  set rogue-event-log [emergency|alert|...]
  set sta-event-log [emergency|alert|...]
  set sta-locate-log [emergency|alert|...]
  set wids-log [emergency|alert|...]
  set wtp-event-log [emergency|alert|...]
end
```

config wireless-controller log

Parameter	Description	Type	Size	Default
status	Enable/disable wireless event logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable wireless event logging.		
	<i>disable</i>	Disable wireless event logging.		
addrgrp-log	Lowest severity level to log address group message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
ble-log	Lowest severity level to log BLE detection message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
clb-log	Lowest severity level to log client load balancing message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
dhcp-starv-log	Lowest severity level to log DHCP starvation event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
led-sched-log	Lowest severity level to log LED schedule event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
radio-event-log	Lowest severity level to log radio event message.	option	-	notification

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
rogue-event-log	Lowest severity level to log rogue AP event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sta-event-log	Lowest severity level to log station event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		

Parameter	Description	Type	Size	Default
sta-locate-log	Lowest severity level to log station locate message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
wids-log	Lowest severity level to log WIDS message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
wtp-event-log	Lowest severity level to log WTP event message.	option	-	notification
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		

config wireless-controller apcfg-profile

Configure AP local configuration profiles.

```
config wireless-controller apcfg-profile
    Description: Configure AP local configuration profiles.
    edit <name>
        set comment {var-string}
        set ac-type [default|specify|...]
        set ac-timer {integer}
        set ac-ip {ipv4-address}
        set ac-port {integer}
        config command-list
            Description: AP local configuration command list.
            edit <id>
                set type [non-password|password]
                set name {string}
                set value {string}
                set passwd-value {password}
            next
        end
    next
end
```

config wireless-controller apcfg-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
ac-type	Validation controller type .	option	-	default
	Option	Description		
	<i>default</i>	This controller is the one and only controller that the AP could join after applying AP local configuration.		
	<i>specify</i>	Specified controller is the one and only controller that the AP could join after applying AP local configuration.		
	<i>apcfg</i>	Any controller defined by AP local configuration after applying AP local configuration.		
ac-timer	Maximum waiting time for the AP to join the validation controller after applying AP local configuration .	integer	Minimum value: 3 Maximum value: 30	10
ac-ip	IP address of the validation controller that AP must be able to join after applying AP local configuration.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
ac-port	Port of the validation controller that AP must be able to join after applying AP local configuration .	integer	Minimum value: 1024 Maximum value: 49150	0

config command-list

Parameter	Description	Type	Size	Default
type	The command type .	option	-	non-password
	Option	Description		
	<i>non-password</i>	Non-password command.		
	<i>password</i>	Password command.		
name	AP local configuration command name.	string	Maximum length: 63	
value	AP local configuration command value.	string	Maximum length: 127	
passwd-value	AP local configuration command password value.	password	Not Specified	

config wireless-controller bonjour-profile

Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour.

```
config wireless-controller bonjour-profile
    Description: Configure Bonjour profiles. Bonjour is Apple's zero configuration networking
                  protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using
                  Bonjour.
    edit <name>
        set comment {string}
        config policy-list
            Description: Bonjour policy list.
            edit <policy-id>
                set description {string}
                set from-vlan {string}
                set to-vlan {string}
                set services {option1}, {option2}, ...
            next
        end
    next
end
```

config wireless-controller bonjour-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	

config policy-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 63	
from-vlan	VLAN ID from which the Bonjour service is advertised .	string	Maximum length: 63	0
to-vlan	VLAN ID to which the Bonjour service is made available .	string	Maximum length: 63	all
services	Bonjour services for the VLAN connecting to the Bonjour network.	option	-	all
Option	Description			
<i>all</i>	All services.			
<i>airplay</i>	AirPlay.			
<i>afp</i>	AFP (Apple File Sharing).			
<i>bit-torrent</i>	BitTorrent.			
<i>ftp</i>	FTP.			
<i>ichat</i>	iChat.			
<i>itunes</i>	iTunes.			
<i>printers</i>	Printers.			
<i>samba</i>	Samba.			
<i>scanners</i>	Scanners.			
<i>ssh</i>	SSH.			
<i>chromecast</i>	ChromeCast.			

config wireless-controller arrp-profile

Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.

```
config wireless-controller arrp-profile
  Description: Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.
  edit <name>
```

```

        set comment {var-string}
        set selection-period {integer}
        set monitor-period {integer}
        set weight-managed-ap {integer}
        set weight-rogue-ap {integer}
        set weight-noise-floor {integer}
        set weight-channel-load {integer}
        set weight-spectral-rssi {integer}
        set weight-weather-channel {integer}
        set weight-dfs-channel {integer}
        set threshold-ap {integer}
        set threshold-noise-floor {string}
        set threshold-channel-load {integer}
        set threshold-spectral-rssi {string}
        set threshold-tx-retries {integer}
        set threshold-rx-errors {integer}
        set include-weather-channel [enable|disable]
        set include-dfs-channel [enable|disable]
    next
end

```

config wireless-controller arrp-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
selection-period	Period in seconds to measure average channel load, noise floor, spectral RSSI .	integer	Minimum value: 0 Maximum value: 65535	3600
monitor-period	Period in seconds to measure average transmit retries and receive errors .	integer	Minimum value: 0 Maximum value: 65535	300
weight-managed-ap	Weight in DARRP channel score calculation for managed APs .	integer	Minimum value: 0 Maximum value: 2000	50
weight-rogue-ap	Weight in DARRP channel score calculation for rogue APs .	integer	Minimum value: 0 Maximum value: 2000	10
weight-noise-floor	Weight in DARRP channel score calculation for noise floor .	integer	Minimum value: 0 Maximum value: 2000	40

Parameter	Description	Type	Size	Default
weight-channel-load	Weight in DARRP channel score calculation for channel load .	integer	Minimum value: 0 Maximum value: 2000	20
weight-spectral-rssi	Weight in DARRP channel score calculation for spectral RSSI .	integer	Minimum value: 0 Maximum value: 2000	40
weight-weather-channel	Weight in DARRP channel score calculation for weather channel .	integer	Minimum value: 0 Maximum value: 2000	1000
weight-dfs-channel	Weight in DARRP channel score calculation for DFS channel .	integer	Minimum value: 0 Maximum value: 2000	500
threshold-ap	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs .	integer	Minimum value: 0 Maximum value: 500	250
threshold-noise-floor	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor .	string	Maximum length: 7	-85
threshold-channel-load	Threshold in percentage to reject channel in DARRP channel selection phase 1 due to channel load .	integer	Minimum value: 0 Maximum value: 100	60
threshold-spectral-rssi	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to spectral RSSI .	string	Maximum length: 7	-65
threshold-tx-retries	Threshold in percentage for transmit retries to trigger channel reselection in DARRP monitor stage .	integer	Minimum value: 0 Maximum value: 1000	300
threshold-rx-errors	Threshold in percentage for receive errors to trigger channel reselection in DARRP monitor stage .	integer	Minimum value: 0 Maximum value: 100	50
include-weather-channel	Enable/disable use of weather channel in DARRP channel selection phase 1 .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Include weather channel in darrp channel selection phase 1.		
	<i>disable</i>	Exclude weather channel in darrp channel selection phase 1.		
include-dfs-channel	Enable/disable use of DFS channel in DARRP channel selection phase 1 .	option	-	disable
	Option	Description		
	<i>enable</i>	Include DFS channel in darrp channel selection phase 1.		
	<i>disable</i>	Exclude DFS channel in darrp channel selection phase 1.		

config wireless-controller region

Configure FortiAP regions (for floor plans and maps).

```
config wireless-controller region
  Description: Configure FortiAP regions (for floor plans and maps).
  edit <name>
    set comments {string}
    set grayscale [enable|disable]
    set opacity {integer}
  next
end
```

config wireless-controller region

Parameter	Description	Type	Size	Default
	Option	Description		
comments	Comments.	string	Maximum length: 1027	
grayscale	Region image grayscale.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable region image grayscale.		
	<i>disable</i>	Disable region image grayscale.		
opacity	Region image opacity .	integer	Minimum value: 0 Maximum value: 100	100

config wireless-controller vap-group

Configure virtual Access Point (VAP) groups.

```
config wireless-controller vap-group
  Description: Configure virtual Access Point (VAP) groups.
  edit <name>
    set comment {var-string}
    set vaps <name1>, <name2>, ...
  next
end
```

config wireless-controller vap-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
vaps <name>	List of SSIDs to be included in the VAP group. vap name	string	Maximum length: 35	

config wireless-controller wids-profile

Configure wireless intrusion detection system (WIDS) profiles.

```
config wireless-controller wids-profile
  Description: Configure wireless intrusion detection system (WIDS) profiles.
  edit <name>
    set comment {string}
    set sensor-mode [disable|foreign|...]
    set ap-scan [disable|enable]
    set ap-bgscan-period {integer}
    set ap-bgscan-intv {integer}
    set ap-bgscan-duration {integer}
    set ap-bgscan-idle {integer}
    set ap-bgscan-report-intv {integer}
    set ap-bgscan-disable-schedules <name1>, <name2>, ...
    set ap-fgscan-report-intv {integer}
    set ap-scan-passive [enable|disable]
    set ap-scan-threshold {string}
    set ap-auto-suppress [enable|disable]
    set wireless-bridge [enable|disable]
    set deauth-broadcast [enable|disable]
    set null-ssid-probe-resp [enable|disable]
    set long-duration-attack [enable|disable]
    set long-duration-thresh {integer}
    set invalid-mac-oui [enable|disable]
    set weak-wep-iv [enable|disable]
    set auth-frame-flood [enable|disable]
    set auth-flood-time {integer}
    set auth-flood-thresh {integer}
    set assoc-frame-flood [enable|disable]
    set assoc-flood-time {integer}
```

```

set assoc-flood-thresh {integer}
set spoofed-deauth [enable|disable]
set asleap-attack [enable|disable]
set eapol-start-flood [enable|disable]
set eapol-start-thresh {integer}
set eapol-start-intv {integer}
set eapol-logoff-flood [enable|disable]
set eapol-logoff-thresh {integer}
set eapol-logoff-intv {integer}
set eapol-succ-flood [enable|disable]
set eapol-succ-thresh {integer}
set eapol-succ-intv {integer}
set eapol-fail-flood [enable|disable]
set eapol-fail-thresh {integer}
set eapol-fail-intv {integer}
set eapol-pre-succ-flood [enable|disable]
set eapol-pre-succ-thresh {integer}
set eapol-pre-succ-intv {integer}
set eapol-pre-fail-flood [enable|disable]
set eapol-pre-fail-thresh {integer}
set eapol-pre-fail-intv {integer}
set deauth-known-src-thresh {integer}
next
end

```

config wireless-controller wids-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	
sensor-mode	Scan nearby WiFi stations .	option	-	disable
Parameter	Description	Option	-	Value
		<i>disable</i>		Disable the scan.
		<i>foreign</i>		Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.
		<i>both</i>		Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.
ap-scan	Enable/disable rogue AP detection.	option	-	disable
Parameter	Description	Option	-	Value
		<i>disable</i>		Disable rogue AP detection.
		<i>enable</i>		Enable rogue AP detection.

Parameter	Description	Type	Size	Default
ap-bgscan-period	Period of time between background scans .	integer	Minimum value: 10 Maximum value: 3600	600
ap-bgscan-intv	Period of time between scanning two channels .	integer	Minimum value: 1 Maximum value: 600	1
ap-bgscan-duration	Listening time on a scanning channel .	integer	Minimum value: 10 Maximum value: 1000	20
ap-bgscan-idle	Waiting time for channel inactivity before scanning this channel .	integer	Minimum value: 0 Maximum value: 1000	0
ap-bgscan-report-intv	Period of time between background scan reports .	integer	Minimum value: 15 Maximum value: 600	30
ap-bgscan-disable-schedules <name>	Firewall schedules for turning off FortiAP radio background scan. Background scan will be disabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35	
ap-fgscan-report-intv	Period of time between foreground scan reports .	integer	Minimum value: 15 Maximum value: 600	15
ap-scan-passive	Enable/disable passive scanning. Enable means do not send probe request on any channels .	option	-	disable
Option	Description			
<i>enable</i>	Passive scanning on all channels.			
<i>disable</i>	Passive scanning only on DFS channels.			
ap-scan-threshold	Minimum signal level/threshold in dBm required for the AP to report detected rogue AP .	string	Maximum length: 7	-90
ap-auto-suppress	Enable/disable on-wire rogue AP auto-suppression .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable on-wire rogue AP auto-suppression.		
	<i>disable</i>	Disable on-wire rogue AP auto-suppression.		
wireless-bridge	Enable/disable wireless bridge detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable wireless bridge detection.		
	<i>disable</i>	Disable wireless bridge detection.		
deauth-broadcast	Enable/disable broadcasting de-authentication detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable broadcast de-authentication detection.		
	<i>disable</i>	Disable broadcast de-authentication detection.		
null-ssid-probe-resp	Enable/disable null SSID probe response detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable null SSID probe resp detection.		
	<i>disable</i>	Disable null SSID probe resp detection.		
long-duration-attack	Enable/disable long duration attack detection based on user configured threshold .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable long duration attack detection.		
	<i>disable</i>	Disable long duration attack detection.		
long-duration-thresh	Threshold value for long duration attack detection .	integer	Minimum value: 1000 Maximum value: 32767	8200
invalid-mac-oui	Enable/disable invalid MAC OUI detection.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable invalid MAC OUI detection.		
	<i>disable</i>	Disable invalid MAC OUI detection.		
weak-wep-iv	Enable/disable weak WEP IV .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable weak WEP IV detection.		
	<i>disable</i>	Disable weak WEP IV detection.		
auth-frame-flood	Enable/disable authentication frame flooding detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable authentication frame flooding detection.		
	<i>disable</i>	Disable authentication frame flooding detection.		
auth-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10
auth-flood-thresh	The threshold value for authentication frame flooding.	integer	Minimum value: 1 Maximum value: 100	30
assoc-frame-flood	Enable/disable association frame flooding detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable association frame flooding detection.		
	<i>disable</i>	Disable association frame flooding detection.		
assoc-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10
assoc-flood-thresh	The threshold value for association frame flooding.	integer	Minimum value: 1 Maximum value: 100	30

Parameter	Description	Type	Size	Default
spoofed-deauth	Enable/disable spoofed de-authentication attack detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable spoofed de-authentication attack detection.		
	<i>disable</i>	Disable spoofed de-authentication attack detection.		
asleep-attack	Enable/disable asleap attack detection .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable asleap attack detection.		
	<i>disable</i>	Disable asleap attack detection.		
eapol-start-flood	Enable/disable EAPOL-Start flooding .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable EAPOL-Start flooding detection.		
	<i>disable</i>	Disable EAPOL-Start flooding detection.		
eapol-start-thresh	The threshold value for EAPOL-Start flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-start-intv	The detection interval for EAPOL-Start flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-logoff-flood	Enable/disable EAPOL-Logoff flooding .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable EAPOL-Logoff flooding detection.		
	<i>disable</i>	Disable EAPOL-Logoff flooding detection.		
eapol-logoff-thresh	The threshold value for EAPOL-Logoff flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10

Parameter	Description	Type	Size	Default
eapol-logoff-intv	The detection interval for EAPOL-Logoff flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-succ-flood	Enable/disable EAPOL-Success flooding .	option	-	disable
Option		Description		
		<i>enable</i> Enable EAPOL-Success flooding detection.		
		<i>disable</i> Disable EAPOL-Success flooding detection.		
eapol-succ-thresh	The threshold value for EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-succ-intv	The detection interval for EAPOL-Success flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-fail-flood	Enable/disable EAPOL-Failure flooding .	option	-	disable
Option		Description		
		<i>enable</i> Enable EAPOL-Failure flooding detection.		
		<i>disable</i> Disable EAPOL-Failure flooding detection.		
eapol-fail-thresh	The threshold value for EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10
eapol-fail-intv	The detection interval for EAPOL-Failure flooding .	integer	Minimum value: 1 Maximum value: 3600	1
eapol-pre-succ-flood	Enable/disable premature EAPOL-Success flooding .	option	-	disable
Option		Description		
		<i>enable</i> Enable premature EAPOL-Success flooding detection.		
		<i>disable</i> Disable premature EAPOL-Success flooding detection.		

Parameter	Description	Type	Size	Default						
eapol-pre-succ-thresh	The threshold value for premature EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable premature EAPOL-Failure flooding detection.</td></tr> <tr> <td><i>disable</i></td><td>Disable premature EAPOL-Failure flooding detection.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable premature EAPOL-Failure flooding detection.	<i>disable</i>	Disable premature EAPOL-Failure flooding detection.
Option	Description									
<i>enable</i>	Enable premature EAPOL-Failure flooding detection.									
<i>disable</i>	Disable premature EAPOL-Failure flooding detection.									
eapol-pre-fail-thresh	The threshold value for premature EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-pre-fail-intv	The detection interval for premature EAPOL-Failure flooding .	integer	Minimum value: 1 Maximum value: 3600	1						
deauth-unknown-src-thresh	Threshold value per second to deauth unknown src for DoS attack (0: no limit).	integer	Minimum value: 0 Maximum value: 65535	10						

config wireless-controller ble-profile

Configure Bluetooth Low Energy profile.

```
config wireless-controller ble-profile
  Description: Configure Bluetooth Low Energy profile.
  edit <name>
    set comment {string}
    set advertising {option1}, {option2}, ...
    set ibeacon-uuid {string}
    set major-id {integer}
    set minor-id {integer}
    set eddystone-namespace {string}
    set eddystone-instance {string}
    set eddystone-url {string}
    set txpower [0|1|...]
    set beacon-interval {integer}
```

```

        set ble-scanning [enable|disable]
    next
end

```

config wireless-controller ble-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	
advertising	Advertising type.	option	-	
	Option	Description		
	<i>ibeacon</i>	iBeacon advertising.		
	<i>eddystone-uid</i>	Eddystone UID advertising.		
	<i>eddystone-url</i>	Eddystone URL advertising.		
ibeacon-uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 63	005ea414-cbd1-11e5-9956-625662870761
major-id	Major ID.	integer	Minimum value: 0 Maximum value: 65535	1000
minor-id	Minor ID.	integer	Minimum value: 0 Maximum value: 65535	2000
eddystone-namespace	Eddystone namespace ID.	string	Maximum length: 10	0102030405
eddystone-instance	Eddystone instance ID.	string	Maximum length: 6	abcdef
eddystone-url	Eddystone URL.	string	Maximum length: 127	http://www.fortinet.com
txpower	Transmit power level .	option	-	0
	Option	Description		
	0	Transmit power level 0 (-21 dBm)		
	1	Transmit power level 1 (-18 dBm)		

Parameter	Description	Type	Size	Default
	Option	Description		
	2	Transmit power level 2 (-15 dBm)		
	3	Transmit power level 3 (-12 dBm)		
	4	Transmit power level 4 (-9 dBm)		
	5	Transmit power level 5 (-6 dBm)		
	6	Transmit power level 6 (-3 dBm)		
	7	Transmit power level 7 (0 dBm)		
	8	Transmit power level 8 (1 dBm)		
	9	Transmit power level 9 (2 dBm)		
	10	Transmit power level 10 (3 dBm)		
	11	Transmit power level 11 (4 dBm)		
	12	Transmit power level 12 (5 dBm)		
beacon-interval	Beacon interval .	integer	Minimum value: 40 Maximum value: 3500	100
ble-scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable BLE scanning.		
	<i>disable</i>	Disable BLE scanning.		

config wireless-controller wtp-profile

Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```
config wireless-controller wtp-profile
  Description: Configure WTP profiles or FortiAP profiles that define radio settings for
    manageable FortiAP platforms.
  edit <name>
    set comment {var-string}
    config platform
      Description: WTP, FortiAP, or AP platform.
      set type [AP-11N|220B|...]
      set mode [single-5G|dual-5G]
      set ddscan [enable|disable]
    end
    set control-message-offload {option1}, {option2}, ...
    set apcfg-profile {string}
    set ble-profile {string}
```

```

set wan-port-mode [wan-lan|wan-only]
config lan
    Description: WTP LAN port mapping.
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
end
set energy-efficient-ethernet [enable|disable]
set led-state [enable|disable]
set led-schedules <name1>, <name2>, ...
set dtls-policy {option1}, {option2}, ...
set dtls-in-kernel [enable|disable]
set max-clients {integer}
set handoff-rssi {integer}
set handoff-sta-thresh {integer}
set handoff-roaming [enable|disable]
config deny-mac-list
    Description: List of MAC addresses that are denied access to this WTP, FortiAP, or AP.
    edit <id>
        set mac {mac-address}
    next
end
set ap-country [--|AF|...]
set ip-fragment-preventing {option1}, {option2}, ...
set tun-mtu-uplink {integer}
set tun-mtu-downlink {integer}
set split-tunneling-acl-path [tunnel|local]
set split-tunneling-acl-local-ap-subnet [enable|disable]
config split-tunneling-acl
    Description: Split tunneling ACL filter list.
    edit <id>
        set dest-ip {ipv4-classnet}
    next
end
set allowaccess {option1}, {option2}, ...
set login-passwd-change [yes|default|...]
set login-passwd {password}
set lldp [enable|disable]
set poe-mode [auto|8023af|...]
set frequency-handoff [enable|disable]

```

```
set ap-handoff [enable|disable]
config radio-1
    Description: Configuration options for radio 1.
    set mode [disabled|ap|...]
    set band [802.11a|802.11b|...]
    set band-5g-type [5g-full|5g-high|...]
    set drma [disable|enable]
    set drma-sensitivity [low|medium|...]
    set airtime-fairness [enable|disable]
    set protection-mode [rtscts|ctsonly|...]
    set powersave-optimize {option1}, {option2}, ...
    set transmit-optimize {option1}, {option2}, ...
    set amsdu [enable|disable]
    set coexistence [enable|disable]
    set zero-wait-dfs [enable|disable]
    set bss-color {integer}
    set short-guard-interval [enable|disable]
    set channel-bonding [160MHz|80MHz|...]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set dtim {integer}
    set beacon-interval {integer}
    set rts-threshold {integer}
    set frag-threshold {integer}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
    set ap-sniffer-ctl [enable|disable]
    set ap-sniffer-data [enable|disable]
    set sam-ssid {string}
    set sam-bssid {mac-address}
    set sam-security-type [open|wpa-personal|...]
    set sam-captive-portal [enable|disable]
    set sam-cwp-username {string}
    set sam-cwp-password {password}
    set sam-cwp-test-url {string}
    set sam-cwp-match-string {string}
    set sam-cwp-success-string {string}
    set sam-cwp-failure-string {string}
    set sam-username {string}
    set sam-password {password}
    set sam-test [ping|iperf]
    set sam-server-type [ip|fqdn]
    set sam-server-ip {ipv4-address}
    set sam-server-fqdn {string}
    set iperf-server-port {integer}
    set iperf-protocol [udp|tcp]
    set sam-report-intv {integer}
    set channel-utilization [enable|disable]
```

```
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-2
    Description: Configuration options for radio 2.
    set mode [disabled|ap|...]
    set band [802.11a|802.11b|...]
    set band-5g-type [5g-full|5g-high|...]
    set drma [disable|enable]
    set drma-sensitivity [low|medium|...]
    set airtime-fairness [enable|disable]
    set protection-mode [rtscts|ctsonly|...]
    set powersave-optimize {option1}, {option2}, ...
    set transmit-optimize {option1}, {option2}, ...
    set amsdu [enable|disable]
    set coexistence [enable|disable]
    set zero-wait-dfs [enable|disable]
    set bss-color {integer}
    set short-guard-interval [enable|disable]
    set channel-bonding [160MHz|80MHz|...]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set dtim {integer}
    set beacon-interval {integer}
    set rts-threshold {integer}
    set frag-threshold {integer}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
    set ap-sniffer-ctl [enable|disable]
    set ap-sniffer-data [enable|disable]
    set sam-ssid {string}
    set sam-bssid {mac-address}
    set sam-security-type [open|wpa-personal|...]
    set sam-captive-portal [enable|disable]
    set sam-cwp-username {string}
    set sam-cwp-password {password}
    set sam-cwp-test-url {string}
    set sam-cwp-match-string {string}
    set sam-cwp-success-string {string}
```

```
set sam-cwp-failure-string {string}
set sam-username {string}
set sam-password {password}
set sam-test [ping|iperf]
set sam-server-type [ip|fqdn]
set sam-server-ip {ipv4-address}
set sam-server-fqdn {string}
set iperf-server-port {integer}
set iperf-protocol [udp|tcp]
set sam-report-intv {integer}
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-3
    Description: Configuration options for radio 3.
    set mode [disabled|ap|...]
    set band [802.11a|802.11b|...]
    set band-5g-type [5g-full|5g-high|...]
    set drma [disable|enable]
    set drma-sensitivity [low|medium|...]
    set airtime-fairness [enable|disable]
    set protection-mode [rtscts|ctsonly|...]
    set powersave-optimize {option1}, {option2}, ...
    set transmit-optimize {option1}, {option2}, ...
    set amsdu [enable|disable]
    set coexistence [enable|disable]
    set zero-wait-dfs [enable|disable]
    set bss-color {integer}
    set short-guard-interval [enable|disable]
    set channel-bonding [160MHz|80MHz|...]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set dtim {integer}
    set beacon-interval {integer}
    set rts-threshold {integer}
    set frag-threshold {integer}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
```

```

set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set sam-ssid {string}
set sam-bssid {mac-address}
set sam-security-type [open|wpa-personal|...]
set sam-captive-portal [enable|disable]
set sam-cwp-username {string}
set sam-cwp-password {password}
set sam-cwp-test-url {string}
set sam-cwp-match-string {string}
set sam-cwp-success-string {string}
set sam-cwp-failure-string {string}
set sam-username {string}
set sam-password {password}
set sam-test [ping|iperf]
set sam-server-type [ip|fqdn]
set sam-server-ip {ipv4-address}
set sam-server-fqdn {string}
set iperf-server-port {integer}
set iperf-protocol [udp|tcp]
set sam-report-intv {integer}
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-4
  Description: Configuration options for radio 4.
  set mode [disabled|ap|...]
  set band [802.11a|802.11b|...]
  set band-5g-type [5g-full|5g-high|...]
  set drma [disable|enable]
  set drma-sensitivity [low|medium|...]
  set airtime-fairness [enable|disable]
  set protection-mode [rtscts|ctsonly|...]
  set powersave-optimize {option1}, {option2}, ...
  set transmit-optimize {option1}, {option2}, ...
  set amsdu [enable|disable]
  set coexistence [enable|disable]
  set zero-wait-dfs [enable|disable]
  set bss-color {integer}
  set short-guard-interval [enable|disable]
  set channel-bonding [160MHz|80MHz|...]
  set auto-power-level [enable|disable]
  set auto-power-high {integer}
  set auto-power-low {integer}
  set auto-power-target {string}
  set power-mode [dBm|percentage]
  set power-level {integer}

```

```

set power-value {integer}
set dtim {integer}
set beacon-interval {integer}
set rts-threshold {integer}
set frag-threshold {integer}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set sam-ssid {string}
set sam-bssid {mac-address}
set sam-security-type [open|wpa-personal|...]
set sam-captive-portal [enable|disable]
set sam-cwp-username {string}
set sam-cwp-password {password}
set sam-cwp-test-url {string}
set sam-cwp-match-string {string}
set sam-cwp-success-string {string}
set sam-cwp-failure-string {string}
set sam-username {string}
set sam-password {password}
set sam-test [ping|iperf]
set sam-server-type [ip|fqdn]
set sam-server-ip {ipv4-address}
set sam-server-fqdn {string}
set iperf-server-port {integer}
set iperf-protocol [udp|tcp]
set sam-report-intv {integer}
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config lbs
Description: Set various location based service (LBS) options.
set ekahau-blink-mode [enable|disable]
set ekahau-tag {mac-address}
set erc-server-ip {ipv4-address-any}
set erc-server-port {integer}
set aeroscout [enable|disable]
set aeroscout-server-ip {ipv4-address-any}
set aeroscout-server-port {integer}
set aeroscout-mu [enable|disable]
set aeroscout-ap-mac [bssid|board-mac]
set aeroscout-mm-report [enable|disable]

```

```

set aeroscout-mu-factor {integer}
set aeroscout-mu-timeout {integer}
set fortipresence [foreign|both|...]
set fortipresence-server {ipv4-address-any}
set fortipresence-port {integer}
set fortipresence-secret {password}
set fortipresence-project {string}
set fortipresence-frequency {integer}
set fortipresence-rogue [enable|disable]
set fortipresence-unassoc [enable|disable]
set fortipresence-ble [enable|disable]
set station-locate [enable|disable]
end
set ext-info-enable [enable|disable]
set indoor-outdoor-deployment [platform-determined|outdoor|...]
config esl-ses-dongle
    Description: ESL SES-imagotag dongle configuration.
    set compliance-level {option}
    set scd-enable [enable|disable]
    set esl-channel [-1|0|...]
    set output-power [a|b|...]
    set apc-addr-type [fqdn|ip]
    set apc-fqdn {string}
    set apc-ip {ipv4-address}
    set apc-port {integer}
    set coex-level {option}
    set tls-cert-verification [enable|disable]
    set tls-fqdn-verification [enable|disable]
end
set console-login [enable|disable]
next
end

```

config wireless-controller wtp-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
control-message-offload	Enable/disable CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.		
	<i>aeroscout-tag</i>	AeroScout tag.		
	<i>ap-list</i>	Rogue AP list.		
	<i>sta-list</i>	Rogue STA list.		
	<i>sta-cap-list</i>	STA capability list.		
	<i>stats</i>	WTP, radio, VAP, and STA statistics.		
	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.		
	<i>sta-health</i>	STA health log.		
	<i>spectral-analysis</i>	Spectral analysis report.		
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35	
ble-profile	Bluetooth Low Energy profile name.	string	Maximum length: 35	
wan-port-mode	Enable/disable using a WAN port as a LAN port.	option	-	wan-only
	Option	Description		
	<i>wan-lan</i>	Enable using a WAN port as a LAN port.		
	<i>wan-only</i>	Disable using a WAN port as a LAN port.		
energy-efficient-ethernet	Enable/disable use of energy efficient Ethernet on WTP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of energy efficient Ethernet on WTP.		
	<i>disable</i>	Disable use of energy efficient Ethernet on WTP.		
led-state	Enable/disable use of LEDs on WTP .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of LEDs on WTP.		
	<i>disable</i>	Disable use of LEDs on WTP.		

Parameter	Description	Type	Size	Default								
led-schedules <name>	Recurring firewall schedules for illuminating LEDs on the FortiAP. If led-state is enabled, LEDs will be visible when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35									
dtls-policy	WTP data channel DTLS policy .	option	-	clear-text								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>clear-text</i></td><td>Clear Text Data Channel.</td></tr> <tr> <td><i>dtls-enabled</i></td><td>DTLS Enabled Data Channel.</td></tr> <tr> <td><i>ipsec-vpn</i></td><td>IPsec VPN Data Channel.</td></tr> </tbody> </table>	Option	Description	<i>clear-text</i>	Clear Text Data Channel.	<i>dtls-enabled</i>	DTLS Enabled Data Channel.	<i>ipsec-vpn</i>	IPsec VPN Data Channel.			
Option	Description											
<i>clear-text</i>	Clear Text Data Channel.											
<i>dtls-enabled</i>	DTLS Enabled Data Channel.											
<i>ipsec-vpn</i>	IPsec VPN Data Channel.											
dtls-in-kernel	Enable/disable data channel DTLS in kernel.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable data channel DTLS in kernel.</td></tr> <tr> <td><i>disable</i></td><td>Disable data channel DTLS in kernel.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable data channel DTLS in kernel.	<i>disable</i>	Disable data channel DTLS in kernel.					
Option	Description											
<i>enable</i>	Enable data channel DTLS in kernel.											
<i>disable</i>	Disable data channel DTLS in kernel.											
max-clients	Maximum number of stations .	integer	Minimum value: 0 Maximum value: 4294967295	0								
handoff-rssi	Minimum received signal strength indicator .	integer	Minimum value: 20 Maximum value: 30	25								
handoff-sta-thresh	Threshold value for AP handoff.	integer	Minimum value: 0 Maximum value: 4294967295	0								
handoff-roaming	Enable/disable client load balancing during roaming to avoid roaming delay .	option	-	enable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable handoff roaming.</td></tr> <tr> <td><i>disable</i></td><td>Disable handoff roaming.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable handoff roaming.	<i>disable</i>	Disable handoff roaming.					
Option	Description											
<i>enable</i>	Enable handoff roaming.											
<i>disable</i>	Disable handoff roaming.											
ap-country	Country in which this WTP, FortiAP or AP will operate .	option	-	--								

Parameter	Description	Type	Size	Default
	Option	Description		
	-	NO_COUNTRY_SET		
	AF	AFGHANISTAN		
	AL	ALBANIA		
	DZ	ALGERIA		
	AS	AMERICAN SAMOA		
	AO	ANGOLA		
	AR	ARGENTINA		
	AM	ARMENIA		
	AU	AUSTRALIA		
	AT	AUSTRIA		
	AZ	AZERBAIJAN		
	BS	BAHAMAS		
	BH	BAHRAIN		
	BD	BANGLADESH		
	BB	BARBADOS		
	BY	BELARUS		
	BE	BELGIUM		
	BZ	BELIZE		
	BJ	BENIN		
	BM	BERMUDA		
	BT	BHUTAN		
	BO	BOLIVIA		
	BA	BOSNIA AND HERZEGOVINA		
	BW	BOTSWANA		
	BR	BRAZIL		
	BN	BRUNEI DARUSSALAM		
	BG	BULGARIA		
	BF	BURKINA-FASO		
	KH	CAMBODIA		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GE</i>	GEORGIA		

Parameter	Description	Type	Size	Default
	Option	Description		
<i>DE</i>	GERMANY			
<i>GH</i>	GHANA			
<i>GI</i>	GIBRALTAR			
<i>GR</i>	GREECE			
<i>GL</i>	GREENLAND			
<i>GD</i>	GRENADA			
<i>GP</i>	GUADELOUPE			
<i>GU</i>	GUAM			
<i>GT</i>	GUATEMALA			
<i>GY</i>	GUYANA			
<i>HT</i>	HAITI			
<i>HN</i>	HONDURAS			
<i>HK</i>	HONG KONG			
<i>HU</i>	HUNGARY			
<i>IS</i>	ICELAND			
<i>IN</i>	INDIA			
<i>ID</i>	INDONESIA			
<i>IQ</i>	IRAQ			
<i>IE</i>	IRELAND			
<i>IM</i>	ISLE OF MAN			
<i>IL</i>	ISRAEL			
<i>IT</i>	ITALY			
<i>CI</i>	COTE_D_IVOIRE			
<i>JM</i>	JAMAICA			
<i>JO</i>	JORDAN			
<i>KZ</i>	KAZAKHSTAN			
<i>KE</i>	KENYA			
<i>KR</i>	KOREA REPUBLIC			
<i>KW</i>	KUWAIT			

Parameter	Description	Type	Size	Default
	Option	Description		
	LA	LAOS		
	LV	LATVIA		
	LB	LEBANON		
	LS	LESOTHO		
	LY	LIBYA		
	LI	LIECHTENSTEIN		
	LT	LITHUANIA		
	LU	LUXEMBOURG		
	MO	MACAU SAR		
	MK	MACEDONIA, FYRO		
	MG	MADAGASCAR		
	MW	MALAWI		
	MY	MALAYSIA		
	MV	MALDIVES		
	ML	MALI		
	MT	MALTA		
	MH	MARSHALL ISLANDS		
	MQ	MARTINIQUE		
	MR	MAURITANIA		
	MU	MAURITIUS		
	YT	MAYOTTE		
	MX	MEXICO		
	FM	MICRONESIA		
	MD	REPUBLIC OF MOLDOVA		
	MC	MONACO		
	MA	MOROCCO		
	MZ	MOZAMBIQUE		
	MM	MYANMAR		
	NA	NAMIBIA		

Parameter	Description	Type	Size	Default
	Option	Description		
	NP	NEPAL		
	NL	NETHERLANDS		
	AN	NETHERLANDS ANTILLES		
	AW	ARUBA		
	NZ	NEW ZEALAND		
	NI	NICARAGUA		
	NE	NIGER		
	NO	NORWAY		
	MP	NORTHERN MARIANA ISLANDS		
	OM	OMAN		
	PK	PAKISTAN		
	PW	PALAU		
	PA	PANAMA		
	PG	PAPUA NEW GUINEA		
	PY	PARAGUAY		
	PE	PERU		
	PH	PHILIPPINES		
	PL	POLAND		
	PT	PORTUGAL		
	PR	PUERTO RICO		
	QA	QATAR		
	RE	REUNION		
	RO	ROMANIA		
	RU	RUSSIA		
	RW	RWANDA		
	BL	SAINT BARTHELEMY		
	KN	SAINT KITTS AND NEVIS		
	LC	SAINT LUCIA		
	MF	SAINT MARTIN		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>PM</i>	SAINT PIERRE AND MIQUELON		
	<i>VC</i>	SAINT VINCENT AND GRENADIENS		
	<i>SA</i>	SAUDI ARABIA		
	<i>SN</i>	SENEGAL		
	<i>RS</i>	REPUBLIC OF SERBIA		
	<i>ME</i>	MONTENEGRO		
	<i>SL</i>	SIERRA LEONE		
	<i>SG</i>	SINGAPORE		
	<i>SK</i>	SLOVAKIA		
	<i>SI</i>	SLOVENIA		
	<i>ZA</i>	SOUTH AFRICA		
	<i>ES</i>	SPAIN		
	<i>LK</i>	SRI LANKA		
	<i>SE</i>	SWEDEN		
	<i>SR</i>	SURINAME		
	<i>CH</i>	SWITZERLAND		
	<i>TW</i>	TAIWAN		
	<i>TZ</i>	TANZANIA		
	<i>TH</i>	THAILAND		
	<i>TG</i>	TOGO		
	<i>TT</i>	TRINIDAD AND TOBAGO		
	<i>TN</i>	TUNISIA		
	<i>TR</i>	TURKEY		
	<i>TM</i>	TURKMENISTAN		
	<i>AE</i>	UNITED ARAB EMIRATES		
	<i>TC</i>	TURKS AND CAICOS		
	<i>UG</i>	UGANDA		
	<i>UA</i>	UKRAINE		
	<i>GB</i>	UNITED KINGDOM		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>US</i>	UNITED STATES2		
	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)		
	<i>UY</i>	URUGUAY		
	<i>UZ</i>	UZBEKISTAN		
	<i>VU</i>	VANUATU		
	<i>VE</i>	VENEZUELA		
	<i>VN</i>	VIET NAM		
	<i>VI</i>	VIRGIN ISLANDS		
	<i>WF</i>	WALLIS AND FUTUNA		
	<i>YE</i>	YEMEN		
	<i>ZM</i>	ZAMBIA		
	<i>ZW</i>	ZIMBABWE		
	<i>JP</i>	JAPAN14		
	<i>CA</i>	CANADA2		
ip-fragment-preventing	Method.	option	-	tcp-mss-adjust
	Option	Description		
	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.		
	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable		
tun-mtu-uplink	The maximum transmission unit .	integer	Minimum value: 576 Maximum value: 1500	0
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel .	integer	Minimum value: 576 Maximum value: 1500	0
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.		
	<i>local</i>	Split tunneling ACL list traffic will be local NATed.		
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-	
	Option	Description		
	<i>https</i>	HTTPS access.		
	<i>ssh</i>	SSH access.		
	<i>snmp</i>	SNMP access.		
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP .	option	-	no
	Option	Description		
	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.		
	<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.		
	<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.		
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified	
lldp	Enable/disable Link Layer Discovery Protocol .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable LLDP.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable LLDP.		
poe-mode	Set the WTP, FortiAP, or AP's PoE mode.	option	-	auto
	Option	Description		
	<i>auto</i>	Automatically detect the PoE mode.		
	<i>8023af</i>	Use 802.3af PoE mode.		
	<i>8023at</i>	Use 802.3at PoE mode.		
	<i>power-adapter</i>	Use the power adapter to control the PoE mode.		
	<i>full</i>	Use full power mode.		
	<i>high</i>	Use high power mode.		
	<i>low</i>	Use low power mode.		
frequency-handoff	Enable/disable frequency handoff of clients to other channels .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable frequency handoff.		
	<i>disable</i>	Disable frequency handoff.		
ap-handoff	Enable/disable AP handoff of clients to other APs .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable AP handoff.		
	<i>disable</i>	Disable AP handoff.		
ext-info-enable	Enable/disable station/VAP/radio extension information.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable station/VAP/radio extension information.		
	<i>disable</i>	Disable station/VAP/radio extension information.		
indoor-outdoor-deployment	Set to allow indoor/outdoor-only channels under regulatory rules .	option	-	platform-determined

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>platform-determined</i>	Set AP deployment type based on its platform.		
	<i>outdoor</i>	Set AP deployment type to outdoor.		
	<i>indoor</i>	Set AP deployment type to indoor.		
console-login	Enable/disable FAP console login access .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FAP console login access.		
	<i>disable</i>	Disable FAP console login access.		

config platform

Parameter	Description	Type	Size	Default
type	WTP, FortiAP or AP platform type. There are built-in WTP profiles for all supported FortiAP models. You can select a built-in profile and customize it or create a new profile.	option	-	221E
	Option	Description		
	<i>AP-11N</i>	Default 11n AP.		
	<i>220B</i>	FAP220B/221B.		
	<i>210B</i>	FAP210B.		
	<i>222B</i>	FAP222B.		
	<i>112B</i>	FAP112B.		
	<i>320B</i>	FAP320B.		
	<i>11C</i>	FAP11C.		
	<i>14C</i>	FAP14C.		
	<i>223B</i>	FAP223B.		
	<i>28C</i>	FAP28C.		
	<i>320C</i>	FAP320C.		
	<i>221C</i>	FAP221C.		
	<i>25D</i>	FAP25D.		

Parameter	Description	Type	Size	Default
Option	Description			
222C	FAP222C.			
224D	FAP224D.			
214B	FK214B.			
21D	FAP21D.			
24D	FAP24D.			
112D	FAP112D.			
223C	FAP223C.			
321C	FAP321C.			
C220C	FAPC220C.			
C225C	FAPC225C.			
C23JD	FAPC23JD.			
C24JE	FAPC24JE.			
S321C	FAPS321C.			
S322C	FAPS322C.			
S323C	FAPS323C.			
S311C	FAPS311C.			
S313C	FAPS313C.			
S321CR	FAPS321CR.			
S322CR	FAPS322CR.			
S323CR	FAPS323CR.			
S421E	FAPS421E.			
S422E	FAPS422E.			
S423E	FAPS423E.			
421E	FAP421E.			
423E	FAP423E.			
221E	FAP221E.			
222E	FAP222E.			
223E	FAP223E.			
224E	FAP224E.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>231E</i>	FAP231E.		
	<i>S221E</i>	FAPS221E.		
	<i>S223E</i>	FAPS223E.		
	<i>321E</i>	FAP321E.		
	<i>431F</i>	FAP431F.		
	<i>432F</i>	FAP432F.		
	<i>433F</i>	FAP433F.		
	<i>231F</i>	FAP231F.		
	<i>234F</i>	FAP234F.		
	<i>23JF</i>	FAP23JF.		
	<i>831F</i>	FAP831F.		
	<i>U421E</i>	FAPU421EV.		
	<i>U422EV</i>	FAPU422EV.		
	<i>U423E</i>	FAPU423EV.		
	<i>U221EV</i>	FAPU221EV.		
	<i>U223EV</i>	FAPU223EV.		
	<i>U24JEV</i>	FAPU24JEV.		
	<i>U321EV</i>	FAPU321EV.		
	<i>U323EV</i>	FAPU323EV.		
	<i>U431F</i>	FAPU431F.		
	<i>U433F</i>	FAPU433F.		
	<i>U231F</i>	FAPU231F.		
	<i>U234F</i>	FAPU234F.		
	<i>U432F</i>	FAPU432F.		
mode	Configure operation mode of 5G radios .	option	-	single-5G
	Option	Description		
	<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.		
	<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.		

Parameter	Description	Type	Size	Default
ddscan	Enable/disable use of one radio for dedicated dual-band scanning to detect RF characterization and wireless threat management.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dedicated dual-band scan mode.		
	<i>disable</i>	Disable dedicated dual-band scan mode.		

config lan

Parameter	Description	Type	Size	Default
port-mode	LAN port mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15	
port1-mode	LAN port 1 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15	
port2-mode	LAN port 2 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		

Parameter	Description	Type	Size	Default
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15	
port3-mode	LAN port 3 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15	
port4-mode	LAN port 4 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15	
port5-mode	LAN port 5 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15	
port6-mode	LAN port 6 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15	
port7-mode	LAN port 7 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15	
port8-mode	LAN port 8 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15	
port-esl-mode	ESL port mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.		
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15	

config deny-mac-list

Parameter	Description	Type	Size	Default
mac	A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.	mac-address	Not Specified	00:00:00:00:00:00

config split-tunneling-acl

Parameter	Description	Type	Size	Default
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0

config radio-1

Parameter	Description	Type	Size	Default
mode	Mode of radio 1. Radio 1 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap
Option		Description		
<i>disabled</i>		Radio 1 is disabled.		
<i>ap</i>		Radio 1 operates as an access point that allows WiFi clients to connect to your network.		
<i>monitor</i>		Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.		
<i>sniffer</i>		Radio 1 operates as a sniffer capturing WiFi frames on air.		
<i>sam</i>		Radio 1 operates as a station that can connect to a neighboring AP for connectivity and health check.		
band	WiFi band that Radio 1 operates on.	option	-	
Option		Description		
<i>802.11a</i>		802.11a.		
<i>802.11b</i>		802.11b.		
<i>802.11g</i>		802.11g/b.		
<i>802.11n</i>		802.11n/g/b at 2.4GHz.		
<i>802.11n-5G</i>		802.11n/a at 5GHz.		
<i>802.11ac</i>		802.11ac/n/a.		
<i>802.11ax-5G</i>		802.11ax/ac/n/a at 5GHz.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.		
	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.		
	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.		
	<i>802.11g-only</i>	802.11g.		
	<i>802.11n-only</i>	802.11n at 2.4GHz.		
	<i>802.11n-5G-only</i>	802.11n at 5GHz.		
	<i>802.11ac,n-only</i>	802.11ac/n.		
	<i>802.11ac-only</i>	802.11ac.		
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.		
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.		
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.		
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.		
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.		
	<i>802.11ax-only</i>	802.11ax at 2.4GHz.		
band-5g-type	WiFi 5G band type.	option	-	5g-full
	Option	Description		
	<i>5g-full</i>	Full 5G band.		
	<i>5g-high</i>	High 5G band.		
	<i>5g-low</i>	Low 5G band.		
drma	Enable/disable dynamic radio mode assignment .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).		
	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).		
drma-sensitivity	Network Coverage Factor .	option	-	low
	Option	Description		
	<i>low</i>	Consider a radio as redundant when its NCF is 100%.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.		
	<i>high</i>	Consider a radio as redundant when its NCF is 90%.		
airtime-fairness	Enable/disable airtime fairness .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable airtime fairness (ATF) support.		
	<i>disable</i>	Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable
	Option	Description		
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-	
	Option	Description		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	Option	Description		
	<i>disable</i>	Disable packet transmission optimization.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .		option	-
	Option	Description		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .		option	-
	Option	Description		
	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.		
	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.		
zero-wait-dfs	Enable/disable zero wait DFS on radio .		option	-
	Option	Description		
	<i>enable</i>	Enable zero wait DFS		
	<i>disable</i>	Disable zero wait DFS		
bss-color	BSS color value for this 11ax radio .		integer	Minimum value: 0 Maximum value: 63
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.		option	-
	Option	Description		
	<i>enable</i>	Select the 400 ns short guard interval (Short GI).		
	<i>disable</i>	Select the 800 ns long guard interval (Long GI).		

Parameter	Description	Type	Size	Default
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz
	Option	Description		
	160MHz	160 MHz channel width.		
	80MHz	80 MHz channel width.		
	40MHz	40 MHz channel width.		
	20MHz	20 MHz channel width.		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable
	Option	Description		
	enable	Enable automatic transmit power adjustment.		
	disable	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	Option	Description		
	dBm	Set radio EIRP power in dBm.		
	percentage	Set radio EIRP power by percentage.		

Parameter	Description	Type	Size	Default
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	36
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable
Option	Description			
<i>enable</i>	Enable sniffer on WiFi management beacon frame.			
<i>disable</i>	Disable sniffer on WiFi management beacon frame.			

Parameter	Description	Type	Size	Default
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi management probe frame.		
	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi management other frame.		
	<i>disable</i>	Disable sniffer on WiFi management other frame.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		
sam-ssid	SSID for WiFi network.	string	Maximum length: 32	
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00
sam-security-type	Select WiFi network security type .	option	-	wpa-personal
	Option	Description		
	<i>open</i>	Open.		
	<i>wpa-personal</i>	WPA/WPA2 personal.		
	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.		

Parameter	Description	Type	Size	Default
sam-captive-portal	Enable/disable Captive Portal Authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Captive Portal Authentication.		
	<i>disable</i>	Disable Captive Portal Authentication.		
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35	
sam-cwp-password	Password for captive portal authentication.	password	Not Specified	
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255	
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64	
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64	
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64	
sam-username	Username for WiFi network connection.	string	Maximum length: 35	
sam-password	Passphrase for WiFi network connection.	password	Not Specified	
sam-test	Select SAM test type .	option	-	ping
	Option	Description		
	<i>ping</i>	PING test.		
	<i>iperf</i>	IPERF test.		
sam-server-type	Select SAM server type .	option	-	ip
	Option	Description		
	<i>ip</i>	IPv4 address.		
	<i>fqdn</i>	Fully Qualified Domain Name address.		
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001						
iperf-protocol	Iperf test protocol .	option	-	udp						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>udp</i></td><td>UDP.</td></tr> <tr> <td><i>tcp</i></td><td>TCP.</td></tr> </tbody> </table>				Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.
Option	Description									
<i>udp</i>	UDP.									
<i>tcp</i>	TCP.									
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0						
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr> <tr> <td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.
Option	Description									
<i>enable</i>	Enable measuring channel utilization.									
<i>disable</i>	Disable measuring channel utilization.									
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr> <tr> <td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr> </tbody> </table>				Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.
Option	Description									
<i>enable</i>	Enable distributed automatic radio resource provisioning.									
<i>disable</i>	Disable distributed automatic radio resource provisioning.									
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0						
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WMM call admission control.		
	<i>disable</i>	Disable WMM call admission control.		
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WMM bandwidth admission control.		
	<i>disable</i>	Disable WMM bandwidth admission control.		
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000

config radio-2

Parameter	Description	Type	Size	Default
mode	Mode of radio 2. Radio 2 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap
	Option	Description		
	<i>disabled</i>	Radio 2 is disabled.		
	<i>ap</i>	Radio 2 operates as an access point that allows WiFi clients to connect to your network.		
	<i>monitor</i>	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.		
	<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.		
	<i>sam</i>	Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.		
band	WiFi band that Radio 2 operates on.	option	-	
	Option	Description		
	<i>802.11a</i>	802.11a.		
	<i>802.11b</i>	802.11b.		
	<i>802.11g</i>	802.11g/b.		
	<i>802.11n</i>	802.11n/g/b at 2.4GHz.		
	<i>802.11n-5G</i>	802.11n/a at 5GHz.		
	<i>802.11ac</i>	802.11ac/n/a.		
	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.		
	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.		
	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.		
	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.		
	<i>802.11g-only</i>	802.11g.		
	<i>802.11n-only</i>	802.11n at 2.4GHz.		
	<i>802.11n-5G-only</i>	802.11n at 5GHz.		
	<i>802.11ac,n-only</i>	802.11ac/n.		
	<i>802.11ac-only</i>	802.11ac.		
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.		
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.		
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.		
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.		
	<i>802.11ax-only</i>	802.11ax at 2.4GHz.		
band-5g-type	WiFi 5G band type.	option	-	5g-full
	Option	Description		
	<i>5g-full</i>	Full 5G band.		
	<i>5g-high</i>	High 5G band.		
	<i>5g-low</i>	Low 5G band.		
drma	Enable/disable dynamic radio mode assignment .	option	-	disable
	Option	Description		
	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).		
	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).		
drma-sensitivity	Network Coverage Factor .	option	-	low
	Option	Description		
	<i>low</i>	Consider a radio as redundant when its NCF is 100%.		
	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.		
	<i>high</i>	Consider a radio as redundant when its NCF is 90%.		
airtime-fairness	Enable/disable airtime fairness .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable airtime fairness (ATF) support.		
	<i>disable</i>	Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>rtscs</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.		-	-
	Option	Description		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.		option	-
	Option	Description		
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .		option	-
	Option	Description		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .		option	-
				enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.		
	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.		
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable zero wait DFS		
	<i>disable</i>	Disable zero wait DFS		
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable
	Option	Description		
	<i>enable</i>	Select the 400 ns short guard interval (Short GI).		
	<i>disable</i>	Select the 800 ns long guard interval (Long GI).		
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz
	Option	Description		
	<i>160MHz</i>	160 MHz channel width.		
	<i>80MHz</i>	80 MHz channel width.		
	<i>40MHz</i>	40 MHz channel width.		
	<i>20MHz</i>	20 MHz channel width.		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		

Parameter	Description	Type	Size	Default
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
Option	Description			
<i>dBm</i>	Set radio EIRP power in dBm.			
<i>percentage</i>	Set radio EIRP power by percentage.			
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100

Parameter	Description	Type	Size	Default						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346						
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	6						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr> <tr> <td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr> <tr> <td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr> <tr> <td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									

Parameter	Description	Type	Size	Default
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		
sam-ssid	SSID for WiFi network.	string	Maximum length: 32	
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00
sam-security-type	Select WiFi network security type .	option	-	wpa-personal
	Option	Description		
	<i>open</i>	Open.		
	<i>wpa-personal</i>	WPA/WPA2 personal.		
	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.		
sam-captive-portal	Enable/disable Captive Portal Authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Captive Portal Authentication.		
	<i>disable</i>	Disable Captive Portal Authentication.		
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35	
sam-cwp-password	Password for captive portal authentication.	password	Not Specified	
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64							
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64							
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64							
sam-username	Username for WiFi network connection.	string	Maximum length: 35							
sam-password	Passphrase for WiFi network connection.	password	Not Specified							
sam-test	Select SAM test type .	option	-	ping						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>ping</i></td><td>PING test.</td></tr> <tr> <td><i>iperf</i></td><td>IPERF test.</td></tr> </tbody> </table>				Option	Description	<i>ping</i>	PING test.	<i>iperf</i>	IPERF test.
Option	Description									
<i>ping</i>	PING test.									
<i>iperf</i>	IPERF test.									
sam-server-type	Select SAM server type .	option	-	ip						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>ip</i></td><td>IPv4 address.</td></tr> <tr> <td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr> </tbody> </table>				Option	Description	<i>ip</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.
Option	Description									
<i>ip</i>	IPv4 address.									
<i>fqdn</i>	Fully Qualified Domain Name address.									
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0						
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255							
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001						
iperf-protocol	Iperf test protocol .	option	-	udp						
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>udp</i></td><td>UDP.</td></tr> <tr> <td><i>tcp</i></td><td>TCP.</td></tr> </tbody> </table>				Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.
Option	Description									
<i>udp</i>	UDP.									
<i>tcp</i>	TCP.									

Parameter	Description	Type	Size	Default
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable
Option		Description		
		<i>enable</i> Enable measuring channel utilization.		
		<i>disable</i> Disable measuring channel utilization.		
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35	
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable
Option		Description		
		<i>enable</i> Enable distributed automatic radio resource provisioning.		
		<i>disable</i> Disable distributed automatic radio resource provisioning.		
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel
Option		Description		
		<i>tunnel</i> Automatically select tunnel SSIDs.		
		<i>bridge</i> Automatically select local-bridging SSIDs.		
		<i>manual</i> Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable
Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable WMM call admission control.		
	<i>disable</i>	Disable WMM call admission control.		
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable
Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable WMM bandwidth admission control.		
	<i>disable</i>	Disable WMM bandwidth admission control.		
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000

config radio-3

Parameter	Description	Type	Size	Default
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap
Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disabled</i>	Radio 3 is disabled.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.		
	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.		
	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.		
	<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.		
band	WiFi band that Radio 3 operates on.	option	-	
	Option	Description		
	<i>802.11a</i>	802.11a.		
	<i>802.11b</i>	802.11b.		
	<i>802.11g</i>	802.11g/b.		
	<i>802.11n</i>	802.11n/g/b at 2.4GHz.		
	<i>802.11n-5G</i>	802.11n/a at 5GHz.		
	<i>802.11ac</i>	802.11ac/n/a.		
	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.		
	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.		
	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.		
	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.		
	<i>802.11g-only</i>	802.11g.		
	<i>802.11n-only</i>	802.11n at 2.4GHz.		
	<i>802.11n-5G-only</i>	802.11n at 5GHz.		
	<i>802.11ac,n-only</i>	802.11ac/n.		
	<i>802.11ac-only</i>	802.11ac.		
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.		
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.		
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.		
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.		
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.		
	<i>802.11ax-only</i>	802.11ax at 2.4GHz.		

Parameter	Description	Type	Size	Default								
band-5g-type	WiFi 5G band type.	option	-	5g-full								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>5g-full</i></td><td>Full 5G band.</td></tr> <tr> <td><i>5g-high</i></td><td>High 5G band.</td></tr> <tr> <td><i>5g-low</i></td><td>Low 5G band.</td></tr> </tbody> </table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.			
Option	Description											
<i>5g-full</i>	Full 5G band.											
<i>5g-high</i>	High 5G band.											
<i>5g-low</i>	Low 5G band.											
drma	Enable/disable dynamic radio mode assignment .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable dynamic radio mode assignment (DRMA).</td></tr> <tr> <td><i>enable</i></td><td>Enable dynamic radio mode assignment (DRMA).</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).					
Option	Description											
<i>disable</i>	Disable dynamic radio mode assignment (DRMA).											
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
drma-sensitivity	Network Coverage Factor .	option	-	low								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>low</i></td><td>Consider a radio as redundant when its NCF is 100%.</td></tr> <tr> <td><i>medium</i></td><td>Consider a radio as redundant when its NCF is 95%.</td></tr> <tr> <td><i>high</i></td><td>Consider a radio as redundant when its NCF is 90%.</td></tr> </tbody> </table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.			
Option	Description											
<i>low</i>	Consider a radio as redundant when its NCF is 100%.											
<i>medium</i>	Consider a radio as redundant when its NCF is 95%.											
<i>high</i>	Consider a radio as redundant when its NCF is 90%.											
airtime-fairness	Enable/disable airtime fairness .	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr> <tr> <td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.					
Option	Description											
<i>enable</i>	Enable airtime fairness (ATF) support.											
<i>disable</i>	Disable airtime fairness (ATF) support.											
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr> <tr> <td><i>ctsonly</i></td><td>Enable 802.11g protection CTS only mode.</td></tr> <tr> <td><i>disable</i></td><td>Disable 802.11g protection mode.</td></tr> </tbody> </table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.			
Option	Description											
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.											
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.											
<i>disable</i>	Disable 802.11g protection mode.											
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	Option	Description		
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.		
	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.		
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable zero wait DFS		

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>disable</i>	Disable zero wait DFS			
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0	
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	enable	
	Option	Description			
	<i>enable</i>	Select the 400 ns short guard interval (Short GI).			
	<i>disable</i>	Select the 800 ns long guard interval (Long GI).			
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz	
	Option	Description			
	<i>160MHz</i>	160 MHz channel width.			
	<i>80MHz</i>	80 MHz channel width.			
	<i>40MHz</i>	40 MHz channel width.			
	<i>20MHz</i>	20 MHz channel width.			
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	enable	
	Option	Description			
	<i>enable</i>	Enable automatic transmit power adjustment.			
	<i>disable</i>	Disable automatic transmit power adjustment.			
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17	

Parameter	Description	Type	Size	Default
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
Option	Description			
<i>dBm</i>	Set radio EIRP power in dBm.			
<i>percentage</i>	Set radio EIRP power by percentage.			
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346

Parameter	Description	Type	Size	Default						
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	6						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr> <tr> <td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management beacon frame.									
<i>disable</i>	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr> <tr> <td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management probe frame.									
<i>disable</i>	Enable sniffer on WiFi management probe frame.									
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr> <tr> <td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi management other frame.									
<i>disable</i>	Disable sniffer on WiFi management other frame.									
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr> <tr> <td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.
Option	Description									
<i>enable</i>	Enable sniffer on WiFi control frame.									
<i>disable</i>	Disable sniffer on WiFi control frame.									
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		
sam-ssid	SSID for WiFi network.	string	Maximum length: 32	
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00
sam-security-type	Select WiFi network security type .	option	-	wpa-personal
	Option	Description		
	<i>open</i>	Open.		
	<i>wpa-personal</i>	WPA/WPA2 personal.		
	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.		
sam-captive-portal	Enable/disable Captive Portal Authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Captive Portal Authentication.		
	<i>disable</i>	Disable Captive Portal Authentication.		
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35	
sam-cwp-password	Password for captive portal authentication.	password	Not Specified	
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255	
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64	
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64	
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64	
sam-username	Username for WiFi network connection.	string	Maximum length: 35	
sam-password	Passphrase for WiFi network connection.	password	Not Specified	

Parameter	Description	Type	Size	Default
sam-test	Select SAM test type .	option	-	ping
	Option	Description		
	<i>ping</i>	PING test.		
	<i>iperf</i>	IPERF test.		
sam-server-type	Select SAM server type .	option	-	ip
	Option	Description		
	<i>ip</i>	IPv4 address.		
	<i>fqdn</i>	Fully Qualified Domain Name address.		
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255	
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001
iperf-protocol	Iperf test protocol .	option	-	udp
	Option	Description		
	<i>udp</i>	UDP.		
	<i>tcp</i>	TCP.		
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable measuring channel utilization.		
	<i>disable</i>	Disable measuring channel utilization.		
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable distributed automatic radio resource provisioning.		
	<i>disable</i>	Disable distributed automatic radio resource provisioning.		
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel
	Option	Description		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WMM call admission control.		
	<i>disable</i>	Disable WMM call admission control.		

Parameter	Description	Type	Size	Default
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable
Option		Description		
		<i>enable</i> Enable WMM bandwidth admission control.		
		<i>disable</i> Disable WMM bandwidth admission control.		
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000

config radio-4

Parameter	Description	Type	Size	Default
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap
Option		Description		
		<i>disabled</i> Radio 3 is disabled.		
		<i>ap</i> Radio 3 operates as an access point that allows WiFi clients to connect to your network.		
		<i>monitor</i> Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.		
		<i>sniffer</i> Radio 3 operates as a sniffer capturing WiFi frames on air.		
		<i>sam</i> Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.		
band	WiFi band that Radio 3 operates on.	option	-	
Option		Description		
		<i>802.11a</i> 802.11a.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>802.11b</i>	802.11b.		
	<i>802.11g</i>	802.11g/b.		
	<i>802.11n</i>	802.11n/g/b at 2.4GHz.		
	<i>802.11n-5G</i>	802.11n/a at 5GHz.		
	<i>802.11ac</i>	802.11ac/n/a.		
	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.		
	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.		
	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.		
	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.		
	<i>802.11g-only</i>	802.11g.		
	<i>802.11n-only</i>	802.11n at 2.4GHz.		
	<i>802.11n-5G-only</i>	802.11n at 5GHz.		
	<i>802.11ac,n-only</i>	802.11ac/n.		
	<i>802.11ac-only</i>	802.11ac.		
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.		
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.		
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.		
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.		
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.		
	<i>802.11ax-only</i>	802.11ax at 2.4GHz.		
band-5g-type	WiFi 5G band type.	option	-	5g-full
	Option	Description		
	<i>5g-full</i>	Full 5G band.		
	<i>5g-high</i>	High 5G band.		
	<i>5g-low</i>	Low 5G band.		
drma	Enable/disable dynamic radio mode assignment .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).		
	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).		
drma-sensitivity	Network Coverage Factor .	option	-	low
	Option	Description		
	<i>low</i>	Consider a radio as redundant when its NCF is 100%.		
	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.		
	<i>high</i>	Consider a radio as redundant when its NCF is 90%.		
airtime-fairness	Enable/disable airtime fairness .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable airtime fairness (ATF) support.		
	<i>disable</i>	Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable
	Option	Description		
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-	
	Option	Description		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		

Parameter	Description	Type	Size	Default												
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>disable</i></td><td>Disable packet transmission optimization.</td></tr> <tr> <td><i>power-save</i></td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr> <tr> <td><i>aggr-limit</i></td><td>Set aggregation limit to a lower value when data rate is low.</td></tr> <tr> <td><i>retry-limit</i></td><td>Set software retry limit to a lower value when data rate is low.</td></tr> <tr> <td><i>send-bar</i></td><td>Limit transmission of BAR frames.</td></tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.			
Option	Description															
<i>disable</i>	Disable packet transmission optimization.															
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.															
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.															
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.															
<i>send-bar</i>	Limit transmission of BAR frames.															
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable AMSDU support.</td></tr> <tr> <td><i>disable</i></td><td>Disable AMSDU support.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.									
Option	Description															
<i>enable</i>	Enable AMSDU support.															
<i>disable</i>	Disable AMSDU support.															
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr> <tr> <td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.									
Option	Description															
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.															
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.															
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-	enable												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable zero wait DFS</td></tr> <tr> <td><i>disable</i></td><td>Disable zero wait DFS</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS									
Option	Description															
<i>enable</i>	Enable zero wait DFS															
<i>disable</i>	Disable zero wait DFS															
bss-color	BSS color value for this 11ax radio .	integer	Minimum value: 0 Maximum value: 63	0												
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Select the 400 ns short guard interval (Short GI).		
	<i>disable</i>	Select the 800 ns long guard interval (Long GI).		
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz
	Option	Description		
	<i>160MHz</i>	160 MHz channel width.		
	<i>80MHz</i>	80 MHz channel width.		
	<i>40MHz</i>	40 MHz channel width.		
	<i>20MHz</i>	20 MHz channel width.		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
dtim	Delivery Traffic Indication Map . Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535	100
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS .	integer	Minimum value: 256 Maximum value: 2346	2346
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346	2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32	16
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295	6
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00

Parameter	Description	Type	Size	Default
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi management beacon frame.		
	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi management probe frame.		
	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi management other frame.		
	<i>disable</i>	Disable sniffer on WiFi management other frame.		
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi control frame.		
	<i>disable</i>	Disable sniffer on WiFi control frame.		
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer on WiFi data frame		
	<i>disable</i>	Disable sniffer on WiFi data frame		
sam-ssid	SSID for WiFi network.	string	Maximum length: 32	
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00
sam-security-type	Select WiFi network security type .	option	-	wpa-personal

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>open</i>	Open.		
	<i>wpa-personal</i>	WPA/WPA2 personal.		
	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.		
sam-captive-portal	Enable/disable Captive Portal Authentication .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Captive Portal Authentication.		
	<i>disable</i>	Disable Captive Portal Authentication.		
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35	
sam-cwp-password	Password for captive portal authentication.	password	Not Specified	
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255	
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64	
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64	
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64	
sam-username	Username for WiFi network connection.	string	Maximum length: 35	
sam-password	Passphrase for WiFi network connection.	password	Not Specified	
sam-test	Select SAM test type .	option	-	ping
	Option	Description		
	<i>ping</i>	PING test.		
	<i>iperf</i>	IPERF test.		
sam-server-type	Select SAM server type .	option	-	ip

Parameter	Description	Type	Size	Default	
	Option	Description			
	<i>ip</i>	IPv4 address.			
	<i>fqdn</i>	Fully Qualified Domain Name address.			
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0	
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255		
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001	
iperf-protocol	Iperf test protocol .	option	-	udp	
	Option	Description			
	<i>udp</i>	UDP.			
	<i>tcp</i>	TCP.			
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0	
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable	
	Option	Description			
	<i>enable</i>	Enable measuring channel utilization.			
	<i>disable</i>	Disable measuring channel utilization.			
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35		
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning .	option	-	disable	
	Option	Description			
	<i>enable</i>	Enable distributed automatic radio resource provisioning.			
	<i>disable</i>	Disable distributed automatic radio resource provisioning.			

Parameter	Description	Type	Size	Default								
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000	0								
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel								
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr> <tr> <td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr> <tr> <td><i>manual</i></td><td>Manually select SSIDs.</td></tr> </tbody> </table>			Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.
Option	Description											
<i>tunnel</i>	Automatically select tunnel SSIDs.											
<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								
		<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Enable WMM call admission control.</td></tr> <tr> <td><i>disable</i></td><td>Disable WMM call admission control.</td></tr> </tbody> </table>			Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.		
Option	Description											
<i>enable</i>	Enable WMM call admission control.											
<i>disable</i>	Disable WMM call admission control.											
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10								

Parameter	Description	Type	Size	Default
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable
Option		Description		
		<code>enable</code> Enable WMM bandwidth admission control.		
		<code>disable</code> Disable WMM bandwidth admission control.		
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000

config lbs

Parameter	Description	Type	Size	Default
ekahau-blink-mode	Enable/disable Ekahau blink mode .	option	-	disable
Option		Description		
		<code>enable</code> Enable Ekahau blink mode.		
		<code>disable</code> Disable Ekahau blink mode.		
ekahau-tag	WiFi frame MAC address or WiFi Tag.	mac-address	Not Specified	01:18:8e:00:00:00
erc-server-ip	IP address of Ekahau RTLS Controller (ERC).	ipv4-address-any	Not Specified	0.0.0.0
erc-server-port	Ekahau RTLS Controller (ERC) UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	8569
aeroscout	Enable/disable AeroScout Real Time Location Service .	option	-	disable
Option		Description		
		<code>enable</code> Enable AeroScout support.		
		<code>disable</code> Disable AeroScout support.		

Parameter	Description	Type	Size	Default
aeroscout-server-ip	IP address of AeroScout server.	ipv4-address-any	Not Specified	0.0.0.0
aeroscout-server-port	AeroScout server UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	0
aeroscout-mu	Enable/disable AeroScout Mobile Unit .	option	-	disable
Option		Description		
		<i>enable</i>	Enable AeroScout MU mode support.	
		<i>disable</i>	Disable AeroScout MU mode support.	
aeroscout-ap-mac	Use BSSID or board MAC address as AP MAC address in AeroScout AP messages	option	-	bssid
Option		Description		
		<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.	
		<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.	
aeroscout-mm-report	Enable/disable compounded AeroScout tag and MU report .	option	-	enable
Option		Description		
		<i>enable</i>	Enable compounded AeroScout tag and MU report.	
		<i>disable</i>	Disable compounded AeroScout tag and MU report.	
aeroscout-mu-factor	AeroScout MU mode dilution factor .	integer	Minimum value: 0 Maximum value: 4294967295	20
aeroscout-mu-timeout	AeroScout MU mode timeout .	integer	Minimum value: 0 Maximum value: 65535	5
fortipresence	Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>foreign</i>	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.		
	<i>both</i>	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.		
	<i>disable</i>	Disable FortiPresence.		
fortipresence-server	FortiPresence server IP address.	ipv4-address-any	Not Specified	0.0.0.0
fortipresence-port	FortiPresence server UDP listening port .	integer	Minimum value: 300 Maximum value: 65535	3000
fortipresence-secret	FortiPresence secret password (max. 16 characters).	password	Not Specified	
fortipresence-project	FortiPresence project name .	string	Maximum length: 16	fortipresence
fortipresence-frequency	FortiPresence report transmit frequency .	integer	Minimum value: 5 Maximum value: 65535	30
fortipresence-rogue	Enable/disable FortiPresence finding and reporting rogue APs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiPresence finding and reporting rogue APs.		
	<i>disable</i>	Disable FortiPresence finding and reporting rogue APs.		
fortipresence-unassoc	Enable/disable FortiPresence finding and reporting unassociated stations.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiPresence finding and reporting unassociated stations.		
	<i>disable</i>	Disable FortiPresence finding and reporting unassociated stations.		
fortipresence-ble	Enable/disable FortiPresence finding and reporting BLE devices.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FortiPresence finding and reporting BLE devices.		
	<i>disable</i>	Disable FortiPresence finding and reporting BLE devices.		
station-locate	Enable/disable client station locating services for all clients, whether associated or not .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable station locating service.		
	<i>disable</i>	Disable station locating service.		

config esl-ses-dongle

Parameter	Description	Type	Size	Default
compliance-level	Compliance levels for the ESL solution integration .	option	-	compliance-level-2
	Option	Description		
	<i>compliance-level-2</i>	Compliance Level 2 - Full Cloud Support, IoT and Fast-Response.		
scd-enable	Enable/disable ESL SES-imagotag Serial Communication Daemon .	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ESL SES-imagotag SCD.		
	<i>disable</i>	Disable ESL SES-imagotag SCD.		
esl-channel	ESL SES-imagotag dongle channel .	option	-	127
	Option	Description		
	<i>-1</i>	No esl-channel is set.		
	<i>0</i>	ESL channel 0.		
	<i>1</i>	ESL channel 1.		
	<i>2</i>	ESL channel 2.		
	<i>3</i>	ESL channel 3.		
	<i>4</i>	ESL channel 4.		

Parameter	Description	Type	Size	Default
	Option	Description		
	5	ESL channel 5.		
	6	ESL channel 6.		
	7	ESL channel 7.		
	8	ESL channel 8.		
	9	ESL channel 9.		
	10	ESL channel 10.		
	127	Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel		
output-power	ESL SES-imagotag dongle output power .	option	-	a
	Option	Description		
	a	About 15mW.		
	b	About 7mW.		
	c	About 5mW.		
	d	About 1mW.		
	e	About 13mW.		
	f	About 10mW.		
	g	About 3mW.		
	h	About 2mW.		
apc-addr-type	ESL SES-imagotag APC address type .	option	-	fqdn
	Option	Description		
	fqdn	Fully Qualified Domain Name address.		
	ip	IPv4 address.		
apc-fqdn	FQDN of ESL SES-imagotag Access Point Controller (APC).	string	Maximum length: 63	
apc-ip	IP address of ESL SES-imagotag Access Point Controller (APC).	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
apc-port	Port of ESL SES-imagotag Access Point Controller (APC).	integer	Minimum value: 0 Maximum value: 65535	0
coex-level	ESL SES-imagotag dongle coexistence level .	option	-	none
Option		Description		
		<i>none</i> No support for coexistence of USB-Dongle with WiFi AP.		
tls-cert-verification	Enable/disable TLS Certificate verification. .	option	-	enable
Option		Description		
		<i>enable</i> Enable TLS Certificate verification.		
		<i>disable</i> Disable TLS Certificate verification.		
tls-fqdn-verification	Enable/disable TLS Certificate verification. .	option	-	disable
Option		Description		
		<i>enable</i> Enable TLS FQDN verification.		
		<i>disable</i> Disable TLS FQDN verification.		

config wireless-controller wtp

Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate.

```
config wireless-controller wtp
  Description: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be
    managed by FortiGate.
  edit <wtp-id>
    set index {integer}
    set uuid {uuid}
    set admin [discovered|disable|...]
    set name {string}
    set location {string}
    set region {string}
    set region-x {string}
    set region-y {string}
    set firmware-provision {string}
    set wtp-profile {string}
    set apcfg-profile {string}
    set bonjour-profile {string}
    set override-led-state [enable|disable]
    set led-state [enable|disable]
    set override-wan-port-mode [enable|disable]
```

```

set wan-port-mode [wan-lan|wan-only]
set override-ip-fragment [enable|disable]
set ip-fragment-preventing {option1}, {option2}, ...
set tun-mtu-uplink {integer}
set tun-mtu-downlink {integer}
set override-split-tunnel [enable|disable]
set split-tunneling-acl-path [tunnel|local]
set split-tunneling-acl-local-ap-subnet [enable|disable]
config split-tunneling-acl
    Description: Split tunneling ACL filter list.
    edit <id>
        set dest-ip {ipv4-classnet}
    next
end
set override-lan [enable|disable]
config lan
    Description: WTP LAN port mapping.
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
end
set override-allowaccess [enable|disable]
set allowaccess {option1}, {option2}, ...
set override-login-passwd-change [enable|disable]
set login-passwd-change [yes|default|...]
set login-passwd {password}
config radio-1
    Description: Configuration options for radio 1.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]

```

```
set vaps <name1>, <name2>, ...
set override-channel [enable|disable]
set channel <chan1>, <chan2>, ...
set drma-manual-mode [ap|monitor|...]
end
config radio-2
    Description: Configuration options for radio 2.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-3
    Description: Configuration options for radio 3.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-4
    Description: Configuration options for radio 4.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
```

```

        set vaps <name1>, <name2>, ...
        set override-channel [enable|disable]
        set channel <chan1>, <chan2>, ...
        set drma-manual-mode [ap|monitor|...]
    end
    set image-download [enable|disable]
    set mesh-bridge-enable [default|enable|...]
    set coordinate-latitude {string}
    set coordinate-longitude {string}
next
end

```

config wireless-controller wtp

Parameter	Description	Type	Size	Default
index	Index .	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
admin	Configure how the FortiGate operating as a wireless controller discovers and manages this WTP, AP or FortiAP.	option	-	enable
Option		Description		
		<i>discovered</i> FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.		
		<i>disable</i> FortiGate wireless controller is configured to not provide service to this WTP.		
		<i>enable</i> FortiGate wireless controller is configured to provide service to this WTP.		
name	WTP, AP or FortiAP configuration name.	string	Maximum length: 35	
location	Field for describing the physical location of the WTP, AP or FortiAP.	string	Maximum length: 35	
region	Region name WTP is associated with.	string	Maximum length: 35	
region-x	Relative horizontal region coordinate (between 0 and 1).	string	Maximum length: 15	0
region-y	Relative vertical region coordinate (between 0 and 1).	string	Maximum length: 15	0

Parameter	Description	Type	Size	Default						
firmware-provision	Firmware version to provision to this FortiAP on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35							
wtp-profile	WTP profile name to apply to this WTP, AP or FortiAP.	string	Maximum length: 35							
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35							
bonjour-profile	Bonjour profile name.	string	Maximum length: 35							
override-led-state	Enable to override the profile LED state setting for this FortiAP. You must enable this option to use the led-state command to turn off the FortiAP's LEDs.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Override the WTP profile LED state.</td></tr> <tr> <td><i>disable</i></td><td>Use the WTP profile LED state.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Override the WTP profile LED state.	<i>disable</i>	Use the WTP profile LED state.
Option	Description									
<i>enable</i>	Override the WTP profile LED state.									
<i>disable</i>	Use the WTP profile LED state.									
led-state	Enable to allow the FortiAPs LEDs to light. Disable to keep the LEDs off. You may want to keep the LEDs off so they are not distracting in low light areas etc.	option	-	enable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Allow the LEDs on this FortiAP to light.</td></tr> <tr> <td><i>disable</i></td><td>Keep the LEDs on this FortiAP off.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Allow the LEDs on this FortiAP to light.	<i>disable</i>	Keep the LEDs on this FortiAP off.
Option	Description									
<i>enable</i>	Allow the LEDs on this FortiAP to light.									
<i>disable</i>	Keep the LEDs on this FortiAP off.									
override-wan-port-mode	Enable/disable overriding the wan-port-mode in the WTP profile.	option	-	disable						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Override the WTP profile wan-port-mode.</td></tr> <tr> <td><i>disable</i></td><td>Use the wan-port-mode in the WTP profile.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Override the WTP profile wan-port-mode.	<i>disable</i>	Use the wan-port-mode in the WTP profile.
Option	Description									
<i>enable</i>	Override the WTP profile wan-port-mode.									
<i>disable</i>	Use the wan-port-mode in the WTP profile.									
wan-port-mode	Enable/disable using the FortiAP WAN port as a LAN port.	option	-	wan-only						
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>wan-lan</i></td><td>Use the FortiAP WAN port as a LAN port.</td></tr> <tr> <td><i>wan-only</i></td><td>Do not use the WAN port as a LAN port.</td></tr> </tbody> </table>					Option	Description	<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.	<i>wan-only</i>	Do not use the WAN port as a LAN port.
Option	Description									
<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.									
<i>wan-only</i>	Do not use the WAN port as a LAN port.									

Parameter	Description	Type	Size	Default
override-ip-fragment	Enable/disable overriding the WTP profile IP fragment prevention setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile IP fragment prevention setting.		
	<i>disable</i>	Use the WTP profile IP fragment prevention setting.		
ip-fragment-preventing	Method.	option	-	tcp-mss-adjust
	Option	Description		
	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.		
	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable		
tun-mtu-uplink	The maximum transmission unit .	integer	Minimum value: 576 Maximum value: 1500	0
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel .	integer	Minimum value: 576 Maximum value: 1500	0
override-split-tunnel	Enable/disable overriding the WTP profile split tunneling setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile split tunneling setting.		
	<i>disable</i>	Use the WTP profile split tunneling setting.		
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local
	Option	Description		
	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.		
	<i>local</i>	Split tunneling ACL list traffic will be local NATed.		
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
override-lan	Enable to override the WTP profile LAN port setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile LAN port setting.		
	<i>disable</i>	Use the WTP profile LAN port setting.		
override-allowaccess	Enable to override the WTP profile management access configuration.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile management access configuration.		
	<i>disable</i>	Use the WTP profile management access configuration.		
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-	
	Option	Description		
	<i>https</i>	HTTPS access.		
	<i>ssh</i>	SSH access.		
	<i>snmp</i>	SNMP access.		
override-login-passwd-change	Enable to override the WTP profile login-password (administrator password) setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile login-password (administrator password) setting.		
	<i>disable</i>	Use the the WTP profile login-password (administrator password) setting.		
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP .	option	-	no

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.		
	<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.		
	<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.		
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified	
image-download	Enable/disable WTP image download.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable WTP image download at join time.		
	<i>disable</i>	Disable WTP image download at join time.		
mesh-bridge-enable	Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.	option	-	default
	Option	Description		
	<i>default</i>	Use mesh Ethernet bridge local setting on the WTP.		
	<i>enable</i>	Turn on mesh Ethernet bridge on the WTP.		
	<i>disable</i>	Turn off mesh Ethernet bridge on the WTP.		
coordinate-latitude	WTP latitude coordinate.	string	Maximum length: 19	
coordinate-longitude	WTP longitude coordinate.	string	Maximum length: 19	

config split-tunneling-acl

Parameter	Description	Type	Size	Default
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config lan

Parameter	Description	Type	Size	Default
port-mode	LAN port mode.	option	-	offline

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15	
port1-mode	LAN port 1 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15	
port2-mode	LAN port 2 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15	
port3-mode	LAN port 3 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		

Parameter	Description	Type	Size	Default
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15	
port4-mode	LAN port 4 mode.	option	-	offline
Option	Description			
<i>offline</i>	Offline.			
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.			
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.			
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15	
port5-mode	LAN port 5 mode.	option	-	offline
Option	Description			
<i>offline</i>	Offline.			
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.			
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.			
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15	
port6-mode	LAN port 6 mode.	option	-	offline
Option	Description			
<i>offline</i>	Offline.			
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.			
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.			
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15	
port7-mode	LAN port 7 mode.	option	-	offline
Option	Description			
<i>offline</i>	Offline.			
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15	
port8-mode	LAN port 8 mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15	
port-esl-mode	ESL port mode.	option	-	offline
	Option	Description		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.		
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15	

config radio-1

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
band	WiFi band that Radio 1 operates on.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>802.11a</i>	802.11a.		
	<i>802.11b</i>	802.11b.		
	<i>802.11g</i>	802.11g/b.		
	<i>802.11n</i>	802.11n/g/b at 2.4GHz.		
	<i>802.11n-5G</i>	802.11n/a at 5GHz.		
	<i>802.11ac</i>	802.11ac/n/a.		
	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.		
	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.		
	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.		
	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.		
	<i>802.11g-only</i>	802.11g.		
	<i>802.11n-only</i>	802.11n at 2.4GHz.		
	<i>802.11n-5G-only</i>	802.11n at 5GHz.		
	<i>802.11ac,n-only</i>	802.11ac/n.		
	<i>802.11ac-only</i>	802.11ac.		
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.		
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.		
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.		
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.		
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.		
	<i>802.11ax-only</i>	802.11ax at 2.4GHz.		
override- txpower	Enable to override the WTP profile power level configuration.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile power level configuration.		
	<i>disable</i>	Use the WTP profile power level configuration.		
auto-power- level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	Option	Description		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel
	Option	Description		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf
	Option	Description		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		

config radio-2

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		

Parameter	Description	Type	Size	Default																																												
band	WiFi band that Radio 2 operates on.	option	-																																													
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>802.11a</i></td><td>802.11a.</td></tr> <tr> <td><i>802.11b</i></td><td>802.11b.</td></tr> <tr> <td><i>802.11g</i></td><td>802.11g/b.</td></tr> <tr> <td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr> <tr> <td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr> <tr> <td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr> <tr> <td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr> <tr> <td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr> <tr> <td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr> <tr> <td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr> <tr> <td><i>802.11g-only</i></td><td>802.11g.</td></tr> <tr> <td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr> <tr> <td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr> <tr> <td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr> <tr> <td><i>802.11ac-only</i></td><td>802.11ac.</td></tr> <tr> <td><i>802.11ax,ac-only</i></td><td>802.11ax/ac at 5GHz.</td></tr> <tr> <td><i>802.11ax,ac,n-only</i></td><td>802.11ax/ac/n at 5GHz.</td></tr> <tr> <td><i>802.11ax-5G-only</i></td><td>802.11ax at 5GHz.</td></tr> <tr> <td><i>802.11ax,n-only</i></td><td>802.11ax/n at 2.4GHz.</td></tr> <tr> <td><i>802.11ax,n,g-only</i></td><td>802.11ax/n/g at 2.4GHz.</td></tr> <tr> <td><i>802.11ax-only</i></td><td>802.11ax at 2.4GHz.</td></tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																																															
<i>802.11a</i>	802.11a.																																															
<i>802.11b</i>	802.11b.																																															
<i>802.11g</i>	802.11g/b.																																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																															
<i>802.11ac</i>	802.11ac/n/a.																																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																															
<i>802.11g-only</i>	802.11g.																																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																															
<i>802.11ac,n-only</i>	802.11ac/n.																																															
<i>802.11ac-only</i>	802.11ac.																																															
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																															
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																															
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																															
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																															
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																															
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																															
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Override the WTP profile power level configuration.</td></tr> <tr> <td><i>disable</i></td><td>Use the WTP profile power level configuration.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.																																									
Option	Description																																															
<i>enable</i>	Override the WTP profile power level configuration.																																															
<i>disable</i>	Use the WTP profile power level configuration.																																															
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable																																												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	Option	Description		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel
	Option	Description		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf
	Option	Description		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		

config radio-3

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		

Parameter	Description	Type	Size	Default																																												
band	WiFi band that Radio 3 operates on.	option	-																																													
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>802.11a</i></td><td>802.11a.</td></tr> <tr> <td><i>802.11b</i></td><td>802.11b.</td></tr> <tr> <td><i>802.11g</i></td><td>802.11g/b.</td></tr> <tr> <td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr> <tr> <td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr> <tr> <td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr> <tr> <td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr> <tr> <td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr> <tr> <td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr> <tr> <td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr> <tr> <td><i>802.11g-only</i></td><td>802.11g.</td></tr> <tr> <td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr> <tr> <td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr> <tr> <td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr> <tr> <td><i>802.11ac-only</i></td><td>802.11ac.</td></tr> <tr> <td><i>802.11ax,ac-only</i></td><td>802.11ax/ac at 5GHz.</td></tr> <tr> <td><i>802.11ax,ac,n-only</i></td><td>802.11ax/ac/n at 5GHz.</td></tr> <tr> <td><i>802.11ax-5G-only</i></td><td>802.11ax at 5GHz.</td></tr> <tr> <td><i>802.11ax,n-only</i></td><td>802.11ax/n at 2.4GHz.</td></tr> <tr> <td><i>802.11ax,n,g-only</i></td><td>802.11ax/n/g at 2.4GHz.</td></tr> <tr> <td><i>802.11ax-only</i></td><td>802.11ax at 2.4GHz.</td></tr> </tbody> </table>					Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.
Option	Description																																															
<i>802.11a</i>	802.11a.																																															
<i>802.11b</i>	802.11b.																																															
<i>802.11g</i>	802.11g/b.																																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																															
<i>802.11ac</i>	802.11ac/n/a.																																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																															
<i>802.11g-only</i>	802.11g.																																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																															
<i>802.11ac,n-only</i>	802.11ac/n.																																															
<i>802.11ac-only</i>	802.11ac.																																															
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																															
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																															
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																															
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																															
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																															
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																															
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																												
<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Override the WTP profile power level configuration.</td></tr> <tr> <td><i>disable</i></td><td>Use the WTP profile power level configuration.</td></tr> </tbody> </table>					Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.																																						
Option	Description																																															
<i>enable</i>	Override the WTP profile power level configuration.																																															
<i>disable</i>	Use the WTP profile power level configuration.																																															
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable																																												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	Option	Description		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel
	Option	Description		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf
	Option	Description		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		

config radio-4

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		

Parameter	Description	Type	Size	Default																																												
band	WiFi band that Radio 4 operates on.	option	-																																													
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>802.11a</i></td><td>802.11a.</td></tr> <tr> <td><i>802.11b</i></td><td>802.11b.</td></tr> <tr> <td><i>802.11g</i></td><td>802.11g/b.</td></tr> <tr> <td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr> <tr> <td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr> <tr> <td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr> <tr> <td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr> <tr> <td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr> <tr> <td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr> <tr> <td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr> <tr> <td><i>802.11g-only</i></td><td>802.11g.</td></tr> <tr> <td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr> <tr> <td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr> <tr> <td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr> <tr> <td><i>802.11ac-only</i></td><td>802.11ac.</td></tr> <tr> <td><i>802.11ax,ac-only</i></td><td>802.11ax/ac at 5GHz.</td></tr> <tr> <td><i>802.11ax,ac,n-only</i></td><td>802.11ax/ac/n at 5GHz.</td></tr> <tr> <td><i>802.11ax-5G-only</i></td><td>802.11ax at 5GHz.</td></tr> <tr> <td><i>802.11ax,n-only</i></td><td>802.11ax/n at 2.4GHz.</td></tr> <tr> <td><i>802.11ax,n,g-only</i></td><td>802.11ax/n/g at 2.4GHz.</td></tr> <tr> <td><i>802.11ax-only</i></td><td>802.11ax at 2.4GHz.</td></tr> </tbody> </table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
Option	Description																																															
<i>802.11a</i>	802.11a.																																															
<i>802.11b</i>	802.11b.																																															
<i>802.11g</i>	802.11g/b.																																															
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																															
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																															
<i>802.11ac</i>	802.11ac/n/a.																																															
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																															
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																															
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																															
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																															
<i>802.11g-only</i>	802.11g.																																															
<i>802.11n-only</i>	802.11n at 2.4GHz.																																															
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																															
<i>802.11ac,n-only</i>	802.11ac/n.																																															
<i>802.11ac-only</i>	802.11ac.																																															
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																																															
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																																															
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																																															
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																																															
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																																															
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																																															
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																												
	<table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><i>enable</i></td><td>Override the WTP profile power level configuration.</td></tr> <tr> <td><i>disable</i></td><td>Use the WTP profile power level configuration.</td></tr> </tbody> </table>	Option	Description	<i>enable</i>	Override the WTP profile power level configuration.	<i>disable</i>	Use the WTP profile power level configuration.																																									
Option	Description																																															
<i>enable</i>	Override the WTP profile power level configuration.																																															
<i>disable</i>	Use the WTP profile power level configuration.																																															
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-	disable																																												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	The target of automatic transmit power adjustment in dBm. .	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power . This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	Option	Description		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power .	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm .	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default
vap-all	Configure method for assigning SSIDs to this FortiAP .	option	-	tunnel
	Option	Description		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode .	option	-	ncf
	Option	Description		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		

config wireless-controller wtp-group

Configure WTP groups.

```
config wireless-controller wtp-group
  Description: Configure WTP groups.
  edit <name>
    set platform-type [AP-11N|220B|...]
    set wtps <wtp-id1>, <wtp-id2>, ...
    next
  end
```

config wireless-controller wtp-group

Parameter	Description	Type	Size	Default
platform-type	FortiAP models to define the WTP group platform type.	option	-	
Option	Description			
AP-11N	Default 11n AP.			
220B	FAP220B/221B.			
210B	FAP210B.			
222B	FAP222B.			
112B	FAP112B.			
320B	FAP320B.			
11C	FAP11C.			
14C	FAP14C.			
223B	FAP223B.			
28C	FAP28C.			
320C	FAP320C.			
221C	FAP221C.			
25D	FAP25D.			
222C	FAP222C.			
224D	FAP224D.			
214B	FK214B.			
21D	FAP21D.			
24D	FAP24D.			
112D	FAP112D.			
223C	FAP223C.			
321C	FAP321C.			
C220C	FAPC220C.			
C225C	FAPC225C.			
C23JD	FAPC23JD.			
C24JE	FAPC24JE.			
S321C	FAPS321C.			
S322C	FAPS322C.			

Parameter	Description	Type	Size	Default
Option	Description			
S323C	FAPS323C.			
S311C	FAPS311C.			
S313C	FAPS313C.			
S321CR	FAPS321CR.			
S322CR	FAPS322CR.			
S323CR	FAPS323CR.			
S421E	FAPS421E.			
S422E	FAPS422E.			
S423E	FAPS423E.			
421E	FAP421E.			
423E	FAP423E.			
221E	FAP221E.			
222E	FAP222E.			
223E	FAP223E.			
224E	FAP224E.			
231E	FAP231E.			
S221E	FAPS221E.			
S223E	FAPS223E.			
321E	FAP321E.			
431F	FAP431F.			
432F	FAP432F.			
433F	FAP433F.			
231F	FAP231F.			
234F	FAP234F.			
23JF	FAP23JF.			
831F	FAP831F.			
U421E	FAPU421EV.			
U422EV	FAPU422EV.			
U423E	FAPU423EV.			

Parameter	Description	Type	Size	Default
Option	Description			
<i>U221EV</i>	FAPU221EV.			
<i>U223EV</i>	FAPU223EV.			
<i>U24JEV</i>	FAPU24JEV.			
<i>U321EV</i>	FAPU321EV.			
<i>U323EV</i>	FAPU323EV.			
<i>U431F</i>	FAPU431F.			
<i>U433F</i>	FAPU433F.			
<i>U231F</i>	FAPU231F.			
<i>U234F</i>	FAPU234F.			
<i>U432F</i>	FAPU432F.			
wtps <wtp-id>	WTP list. WTP ID.	string	Maximum length: 35	

config wireless-controller qos-profile

Configure WiFi quality of service (QoS) profiles.

```
config wireless-controller qos-profile
  Description: Configure WiFi quality of service (QoS) profiles.
  edit <name>
    set comment {string}
    set uplink {integer}
    set downlink {integer}
    set uplink-sta {integer}
    set downlink-sta {integer}
    set burst [enable|disable]
    set wmm [enable|disable]
    set wmm-uapsd [enable|disable]
    set call-admission-control [enable|disable]
    set call-capacity {integer}
    set bandwidth-admission-control [enable|disable]
    set bandwidth-capacity {integer}
    set dscp-wmm-mapping [enable|disable]
    set dscp-wmm-vo <id1>, <id2>, ...
    set dscp-wmm-vi <id1>, <id2>, ...
    set dscp-wmm-be <id1>, <id2>, ...
    set dscp-wmm-bk <id1>, <id2>, ...
    set wmm-dscp-marking [enable|disable]
    set wmm-vo-dscp {integer}
    set wmm-vi-dscp {integer}
    set wmm-be-dscp {integer}
    set wmm-bk-dscp {integer}
  next
```

end

config wireless-controller qos-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	
uplink	Maximum uplink bandwidth for Virtual Access Points .	integer	Minimum value: 0 Maximum value: 2097152	0
downlink	Maximum downlink bandwidth for Virtual Access Points	integer	Minimum value: 0 Maximum value: 2097152	0
uplink-sta	Maximum uplink bandwidth for clients .	integer	Minimum value: 0 Maximum value: 2097152	0
downlink-sta	Maximum downlink bandwidth for clients .	integer	Minimum value: 0 Maximum value: 2097152	0
burst	Enable/disable client rate burst.	option	-	disable
Option	Description			
<i>enable</i>	Enable client rate burst.			
<i>disable</i>	Disable client rate burst.			
wmm	Enable/disable WiFi multi-media (WMM) control.	option	-	enable
Option	Description			
<i>enable</i>	Enable WiFi multi-media (WMM) control.			
<i>disable</i>	Disable WiFi multi-media (WMM) control.			
wmm-uapsd	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.		
	<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.		
call-admission-control	Enable/disable WMM call admission control.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WMM call admission control.		
	<i>disable</i>	Disable WMM call admission control.		
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60	10
bandwidth-admission-control	Enable/disable WMM bandwidth admission control.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WMM bandwidth admission control.		
	<i>disable</i>	Disable WMM bandwidth admission control.		
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000	2000
dscp-wmm-mapping	Enable/disable Differentiated Services Code Point (DSCP) mapping.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Differentiated Services Code Point (DSCP) mapping.		
	<i>disable</i>	Disable Differentiated Services Code Point (DSCP) mapping.		
dscp-wmm-vo <id>	DSCP mapping for voice access (default = 48 56). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63	

Parameter	Description	Type	Size	Default
dscp-wmm-vi <id>	DSCP mapping for video access (default = 32 40). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63	
dscp-wmm-be <id>	DSCP mapping for best effort access (default = 0 24). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63	
dscp-wmm-bk <id>	DSCP mapping for background access (default = 8 16). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63	
wmm-dscp-marking	Enable/disable WMM Differentiated Services Code Point (DSCP) marking.	option	-	disable
Option	Description			
enable	Enable WMM Differentiated Services Code Point (DSCP) marking.			
disable	Disable WMM Differentiated Services Code Point (DSCP) marking.			
wmm-vo-dscp	DSCP marking for voice access .	integer	Minimum value: 0 Maximum value: 63	48
wmm-vi-dscp	DSCP marking for video access .	integer	Minimum value: 0 Maximum value: 63	32
wmm-be-dscp	DSCP marking for best effort access .	integer	Minimum value: 0 Maximum value: 63	0
wmm-bk-dscp	DSCP marking for background access .	integer	Minimum value: 0 Maximum value: 63	8

config wireless-controller wag-profile

Configure wireless access gateway (WAG) profiles used for tunnels on AP.

```
config wireless-controller wag-profile
  Description: Configure wireless access gateway (WAG) profiles used for tunnels on AP.
  edit <name>
    set comment {var-string}
```

```

set tunnel-type [l2tpv3|gre]
set wag-ip {ipv4-address}
set wag-port {integer}
set ping-interval {integer}
set ping-number {integer}
set return-packet-timeout {integer}
set dhcp-ip-addr {ipv4-address}
next
end

```

config wireless-controller wag-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
	Option	Description		
tunnel-type	Tunnel type.	option	-	l2tpv3
	/2tpv3	L2TPV3 Ethernet Pseudowire.		
	gre	GRE Ethernet tunnel.		
wag-ip	IP Address of the wireless access gateway.	ipv4-address	Not Specified	0.0.0.0
wag-port	UDP port of the wireless access gateway.	integer	Minimum value: 0 Maximum value: 65535	1701
ping-interval	Interval between two tunnel monitoring echo packets .	integer	Minimum value: 1 Maximum value: 65535	1
ping-number	Number of the tunnel monitoring echo packets .	integer	Minimum value: 1 Maximum value: 65535	5
return-packet-timeout	Window of time for the return packets from the tunnel's remote end .	integer	Minimum value: 1 Maximum value: 65535	160
dhcp-ip-addr	IP address of the monitoring DHCP request packet sent through the tunnel	ipv4-address	Not Specified	0.0.0.0

config wireless-controller utm-profile

Configure UTM (Unified Threat Management) profile.

```
config wireless-controller utm-profile
  Description: Configure UTM (Unified Threat Management) profile.
  edit <name>
    set comment {string}
    set utm-log [enable|disable]
    set ips-sensor {string}
    set application-list {string}
    set antivirus-profile {string}
    set webfilter-profile {string}
    set scan-botnet-connections [disable|monitor|...]
  next
end
```

config wireless-controller utm-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	
utm-log	Enable/disable UTM logging.	option	-	enable
Option		Description		
		<i>enable</i> Enable UTM logging.		
		<i>disable</i> Disable UTM logging.		
ips-sensor	IPS sensor name.	string	Maximum length: 35	
application-list	Application control list name.	string	Maximum length: 35	
antivirus-profile	AntiVirus profile name.	string	Maximum length: 35	
webfilter-profile	WebFilter profile name.	string	Maximum length: 35	
scan-botnet-connections	Block or monitor connections to Botnet servers or disable Botnet scanning.	option	-	monitor
Option		Description		
		<i>disable</i> Do not scan connections to botnet servers.		
		<i>monitor</i> Log connections to botnet servers.		
		<i>block</i> Block connections to botnet servers.		

config wireless-controller address

Configure the client with its MAC address.

```
config wireless-controller address
  Description: Configure the client with its MAC address.
  edit <id>
    set mac {mac-address}
    set policy [allow|deny]
  next
end
```

config wireless-controller address

Parameter	Description	Type	Size	Default
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
policy	Allow or block the client with this MAC address.	option	-	deny
Option	Description			
<i>allow</i>		Allow the client with this MAC address.		
<i>deny</i>		Block the client with this MAC address.		

config wireless-controller addrgrp

Configure the MAC address group.

```
config wireless-controller addrgrp
  Description: Configure the MAC address group.
  edit <id>
    set default-policy [allow|deny]
    set addresses <id1>, <id2>, ...
  next
end
```

config wireless-controller addrgrp

Parameter	Description	Type	Size	Default
default-policy	Allow or block the clients with MAC addresses that are not in the group.	option	-	allow
Option	Description			
<i>allow</i>		Allow the clients with MAC addresses that are not in the group.		
<i>deny</i>		Block the clients with MAC addresses that are not in the group.		

Parameter	Description	Type	Size	Default
addresses <id>	Manually selected group of addresses. Address ID.	string	Maximum length: 35	

config wireless-controller snmp

Configure SNMP.

```
config wireless-controller snmp
    Description: Configure SNMP.
    set engine-id {string}
    set contact-info {string}
    set trap-high-cpu-threshold {integer}
    set trap-high-mem-threshold {integer}
    config community
        Description: SNMP Community Configuration.
        edit <id>
            set name {string}
            set status [enable|disable]
            set query-v1-status [enable|disable]
            set query-v2c-status [enable|disable]
            set trap-v1-status [enable|disable]
            set trap-v2c-status [enable|disable]
            config hosts
                Description: Configure IPv4 SNMP managers (hosts).
                edit <id>
                    set ip {user}
                next
            end
        next
    end
    config user
        Description: SNMP User Configuration.
        edit <name>
            set status [enable|disable]
            set queries [enable|disable]
            set trap-status [enable|disable]
            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}
            set notify-hosts {ipv4-address}
        next
    end
end
```

config wireless-controller snmp

Parameter	Description	Type	Size	Default
engine-id	AC SNMP enginelid string (maximum 24 characters).	string	Maximum length: 23	
contact-info	Contact Information.	string	Maximum length: 31	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80
trap-high-mem-threshold	Memory usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80

config community

Parameter	Description	Type	Size	Default
name	Community name.	string	Maximum length: 35	
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-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
Option		Description		
		<i>enable</i>		Enable setting.
		<i>disable</i>		Disable setting.
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config hosts

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

config user

Parameter	Description	Type	Size	Default
status	SNMP User Enable	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
queries	Enable/disable SNMP queries for this user.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trap-status	Enable/disable traps for this SNMP user.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
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.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes
	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	
notify-hosts	Configure SNMP User Notify Hosts.	ipv4-address	Not Specified	

config wireless-controller mpsk-profile

Configure MPSK profile.

```
config wireless-controller mpsk-profile
  Description: Configure MPSK profile.
  edit <name>
    set mpsk-concurrent-clients {integer}
    config mpsk-group
      Description: List of multiple PSK groups.
      edit <name>
        set vlan-type [no-vlan|fixed-vlan]
        set vlan-id {integer}
        config mpsk-key
          Description: List of multiple PSK entries.
```

```

        edit <name>
            set mac {mac-address}
            set passphrase {password}
            set concurrent-client-limit-type [default|unlimited|...]
            set concurrent-clients {integer}
            set comment {var-string}
            set mpsk-schedules <name1>, <name2>, ...
        next
    end
next
end
next
end
next
end

```

config wireless-controller mpsk-profile

Parameter	Description	Type	Size	Default
mpsk-concurrent-clients	Maximum number of concurrent clients that connect using the same passphrase in multiple PSK authentication .	integer	Minimum value: 0 Maximum value: 65535	0

config mpsk-group

Parameter	Description	Type	Size	Default
vlan-type	MPSK group VLAN options.	option	-	no-vlan
Option		Description		
		no-vlan No VLAN.		
		fixed-vlan Fixed VLAN ID.		
vlan-id	Optional VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0

config mpsk-key

Parameter	Description	Type	Size	Default
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
passphrase	WPA Pre-shared key.	password	Not Specified	

Parameter	Description	Type	Size	Default
concurrent-client-limit-type	MPSK client limit type options.	option	-	default
	Option	Description		
	<i>default</i>	Using the value in profile configuration.		
	<i>unlimited</i>	Unlimited.		
	<i>specified</i>	Specified value.		
concurrent-clients	Number of clients that can connect using this pre-shared key .	integer	Minimum value: 1 Maximum value: 65535	256
comment	Comment.	var-string	Maximum length: 255	
mpsk-schedules <name>	Firewall schedule for MPSK passphrase. The passphrase will be effective only when at least one schedule is valid. Schedule name.	string	Maximum length: 35	

config wireless-controller nac-profile

Configure WiFi network access control (NAC) profiles.

```
config wireless-controller nac-profile
  Description: Configure WiFi network access control (NAC) profiles.
  edit <name>
    set comment {var-string}
    set onboarding-vlan {string}
  next
end
```

config wireless-controller nac-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
onboarding-vlan	VLAN interface name.	string	Maximum length: 35	

config wireless-controller ssid-policy

Configure WiFi SSID policies.

```
config wireless-controller ssid-policy
  Description: Configure WiFi SSID policies.
  edit <name>
    set description {var-string}
    set vlan {string}
  next
end
```

config wireless-controller ssid-policy

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
vlan	VLAN interface name.	string	Maximum length: 35	

config wireless-controller access-control-list

Configure WiFi bridge access control list.

```
config wireless-controller access-control-list
  Description: Configure WiFi bridge access control list.
  edit <name>
    set comment {string}
    config layer3-ipv4-rules
      Description: AP ACL layer3 ipv4 rule list.
      edit <rule-id>
        set comment {string}
        set srcaddr {user}
        set srcport {integer}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set action [allow|deny]
      next
    end
    config layer3-ipv6-rules
      Description: AP ACL layer3 ipv6 rule list.
      edit <rule-id>
        set comment {string}
        set srcaddr {user}
        set srcport {integer}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set action [allow|deny]
      next
    end
```

```
next  
end
```

config wireless-controller access-control-list

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	

config layer3-ipv4-rules

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	
srcaddr	Source IP address .	user	Not Specified	
srcport	Source port .	integer	Minimum value: 0 Maximum value: 65535	0
dstaddr	Destination IP address .	user	Not Specified	
dstport	Destination port .	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	255
action	Policy action (allow deny).	option	-	

Option	Description
allow	Allows traffic matching the policy.
deny	Blocks traffic matching the policy.

config layer3-ipv6-rules

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	
srcaddr	Source IPv6 address (any local-LAN IPv6 address [/prefix length]), default = any.	user	Not Specified	
srcport	Source port .	integer	Minimum value: 0 Maximum value: 65535	0
dstaddr	Destination IPv6 address (any local-LAN IPv6 address [/prefix length]), default = any.	user	Not Specified	
dstport	Destination port .	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255	255
action	Policy action (allow deny).	option	-	

Option	Description
allow	Allows traffic matching the policy.
deny	Blocks traffic matching the policy.

config wireless-controller scan

Wireless controller scan result.

```
config wireless-controller scan
  Description: Wireless controller scan result.
end
```

config wireless-controller ap-status

Configure access point status (rogue | accepted | suppressed).

```
config wireless-controller ap-status
  Description: Configure access point status (rogue | accepted | suppressed).
  edit <id>
    set bssid {mac-address}
```

```

        set ssid {string}
        set status [rogue|accepted|...]
    next
end

```

config wireless-controller ap-status

Parameter	Description	Type	Size	Default
bssid	Access Point's (AP's) BSSID.	mac-address	Not Specified	00:00:00:00:00:00
ssid	Access Point's (AP's) SSID.	string	Maximum length: 32	
status	Access Point's (AP's) status: rogue, accepted, or suppressed.	option	-	rogue
	Option	Description		
	<i>rogue</i>	Rogue AP.		
	<i>accepted</i>	Accepted AP.		
	<i>suppressed</i>	Suppressed AP.		

config wireless-controller wlchanlistlic

Get channel list according to the region code.

```

config wireless-controller wlchanlistlic
    Description: Get channel list according to the region code.
end

```

config wireless-controller status

Wireless controller status.

```

config wireless-controller status
    Description: Wireless controller status.
    set [1|2] {string}
end

```

config wireless-controller status

Parameter	Description	Type	Size	Default
[1 2]	verbose	string	Maximum length: -1	

config wireless-controller wtp-status

Wireless controller WTP-status.

```
config wireless-controller wtp-status
    Description: Wireless controller WTP-status.
    set <wtp-id> {string}
end
```

config wireless-controller wtp-status

Parameter	Description	Type	Size	Default
<wtp-id>	WTP ID.	string	Maximum length: -1	

config wireless-controller client-info

Wireless controller client-info.

```
config wireless-controller client-info
    Description: Wireless controller client-info.
    set <vfid> {string}
end
```

config wireless-controller client-info

Parameter	Description	Type	Size	Default
<vfid>	VFID.	string	Maximum length: -1	

config wireless-controller vap-status

Wireless controller VAP-status.

```
config wireless-controller vap-status
    Description: Wireless controller VAP-status.
    set [1] {string}
end
```

config wireless-controller vap-status

Parameter	Description	Type	Size	Default
[1]	verbose	string	Maximum length: -1	

config wireless-controller rf-analysis

Wireless controller rf-analysis.

```
config wireless-controller rf-analysis
    Description: Wireless controller rf-analysis.
    set <wtp-id> {string}
end
```

config wireless-controller rf-analysis

Parameter	Description	Type	Size	Default
<wtp-id>	WTP ID.	string	Maximum length: -1	

config wireless-controller spectral-info

Wireless controller spectrum analysis.

```
config wireless-controller spectral-info
    Description: Wireless controller spectrum analysis.
    set [wtp-id] {string}
end
```

config wireless-controller spectral-info

Parameter	Description	Type	Size	Default
[wtp-id]	WTP ID.	string	Maximum length: -1	



www.fortinet.com

Copyright© 2021 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 General Counsel, 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.