FortiOS - CLI Reference

Version 6.2.9

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 19, 2021
FortiOS 6.2.9 CLI Reference
01-629-685877-20210719

TABLE OF CONTENTS

Change Log **17**
FortiOS CLI reference **18**
Availability of commands and options 18
CLI configuration commands **19**
alertemail 20
config alertemail setting 20
antivirus 26
config antivirus settings 26
config antivirus heuristic 27
config antivirus quarantine 27
config antivirus profile 32
application 56
config application name 56
config application custom 58
config application rule-settings 58
config application list 59
config application group 66
authentication 68
config authentication scheme 68
config authentication rule 69
config authentication setting 71
certificate 73
config certificate ca 73
config certificate remote 74
config certificate local 75
config certificate crl 78
cifs 80
config cifs domain-controller 80
config cifs profile 80
dlp 83
config dlp filepattern 83
config dlp sensitivity 86
config dlp sensor 86
dnsfilter 91
config dnsfilter domain-filter 91
config dnsfilter profile 92
emailfilter 97
config emailfilter bword 97
config emailfilter bwl 99
config emailfilter mheader 101
config emailfilter dnsbl 102
config emailfilter iptrust 103
config emailfilter profile 104
config emailfilter fortishield 112

config emailfilter options 113
endpoint-control 114
config endpoint-control settings 114
config endpoint-control fctems 115
extender 117
config extender sys-info 117
config extender modem-status 117
extender-controller 118
config extender-controller extender 118
firewall 124
config firewall address 126
config firewall multicast-address 130
config firewall address6-template 131
config firewall address6 132
config firewall multicast-address6 135
config firewall addrgrp 136
config firewall addrgrp6 138
config firewall wildcard-fqdn custom 139
config firewall wildcard-fqdn group 140
config firewall service category 141
config firewall service custom 141
config firewall service group 145
config firewall internet-service 146
config firewall internet-service-group 148
config firewall internet-service-extension 148
config firewall internet-service-reputation 150
config firewall internet-service-custom 151
config firewall internet-service-addition 152
config firewall internet-service-append 153
config firewall internet-service-custom-group 154
config firewall internet-service-sld 154
config firewall internet-service-ipbl-vendor 155
config firewall internet-service-ipbl-reason 155
config firewall internet-service-owner 155
config firewall internet-service-list 156
config firewall internet-service-definition 156
config firewall shaper traffic-shaper 157
config firewall shaper per-ip-shaper 159
config firewall shaper traffic 161
config firewall shaper per-ip 161
config firewall proxy-address 161
config firewall proxy-addrgrp 164
config firewall schedule onetime 166
config firewall schedule recurring 166
config firewall schedule group 167
config firewall ippool 168
config firewall ippool6 170
config firewall ldb-monitor 170
config firewall vip 171

config firewall vip46 ... 198
config firewall vip6 ... 202
config firewall vip64 ... 227
config firewall vipgrp ... 230
config firewall vipgrp46 ... 231
config firewall vipgrp6 ... 232
config firewall vipgrp64 ... 232
config firewall ipmacbinding setting ... 233
config firewall ipmacbinding table ... 234
config firewall profile-protocol-options ... 235
config firewall ssl-ssh-profile ... 253
config firewall profile-group ... 269
config firewall ssl-server ... 270
config firewall identity-based-route ... 272
config firewall auth-portal ... 273
config firewall consolidated policy ... 274
config firewall security-policy ... 283
config firewall policy ... 289
config firewall traffic-class ... 306
config firewall shaping-policy ... 307
config firewall shaping-profile ... 311
config firewall local-in-policy ... 313
config firewall policy6 ... 315
config firewall local-in-policy6 ... 325
config firewall ttl-policy ... 326
config firewall policy64 ... 327
config firewall policy46 ... 330
config firewall proxy-policy ... 333
config firewall dnstranslation ... 339
config firewall multicast-policy ... 339
config firewall multicast-policy6 ... 341
config firewall interface-policy ... 343
config firewall interface-policy6 ... 346
config firewall DoS-policy ... 349
config firewall DoS-policy6 ... 351
config firewall sniffer ... 353
config firewall central-snat-map ... 358
config firewall ssl setting ... 360
config firewall ssh local-key ... 361
config firewall ssh local-ca ... 362
config firewall ssh setting ... 363
config firewall ssh host-key ... 364
config firewall ip-translation ... 365
config firewall ipv6-eh-filter ... 366
config firewall iprope list ... 368
config firewall iprope appctrl list ... 368
config firewall iprope appctrl status ... 368
config firewall proute ... 368
config firewall proute6 ... 369

ftp-proxy ... 370
config ftp-proxy explicit ... 370
hardware ... 372
config hardware status ... 372
config hardware cpu ... 372
config hardware memory ... 372
config hardware nic ... 372
icap ... 374
config icap server ... 374
config icap profile ... 375
ips ... 379
config ips sensor ... 379
config ips view-map ... 387
config ips decoder ... 388
config ips rule ... 388
config ips rule-settings ... 390
config ips custom ... 390
config ips global ... 392
config ips settings ... 396
config ips session ... 397
ipsec ... 398
config ipsec tunnel ... 398
log ... 399
config log threat-weight ... 400
config log custom-field ... 410
config log syslogd setting ... 410
config log syslogd override-setting ... 414
config log syslogd filter ... 417
config log syslogd override-filter ... 419
config log syslogd2 setting ... 421
config log syslogd2 override-setting ... 425
config log syslogd2 filter ... 428
config log syslogd2 override-filter ... 430
config log syslogd3 setting ... 432
config log syslogd3 override-setting ... 436
config log syslogd3 filter ... 439
config log syslogd3 override-filter ... 441
config log syslogd4 setting ... 443
config log syslogd4 override-setting ... 447
config log syslogd4 filter ... 450
config log syslogd4 override-filter ... 452
config log webtrends setting ... 454
config log webtrends filter ... 455
config log memory global-setting ... 456
config log memory setting ... 457
config log memory filter ... 458
config log disk setting ... 463
config log disk filter ... 467
config log eventfilter ... 472

config log fortiguard setting ... 475
config log fortiguard override-setting ... 477
config log fortiguard filter ... 478
config log fortiguard override-filter ... 480
config log null-device setting ... 482
config log null-device filter ... 483
config log setting ... 484
config log gui-display ... 488
config log fortianalyzer setting ... 489
config log fortianalyzer override-setting ... 493
config log fortianalyzer filter ... 497
config log fortianalyzer override-filter ... 499
config log fortianalyzer2 setting ... 501
config log fortianalyzer2 override-setting ... 505
config log fortianalyzer2 filter ... 509
config log fortianalyzer2 override-filter ... 511
config log fortianalyzer3 setting ... 513
config log fortianalyzer3 override-setting ... 517
config log fortianalyzer3 filter ... 521
config log fortianalyzer3 override-filter ... 523
config log fortianalyzer-cloud setting ... 525
config log fortianalyzer-cloud override-setting ... 528
config log fortianalyzer-cloud filter ... 528
config log fortianalyzer-cloud override-filter ... 530
mgmt-data ... 533
config mgmt-data status ... 533
router ... 534
config router access-list ... 534
config router access-list6 ... 535
config router aspath-list ... 536
config router prefix-list ... 537
config router prefix-list6 ... 538
config router key-chain ... 539
config router community-list ... 540
config router route-map ... 541
config router rip ... 547
config router ripng ... 552
config router static ... 557
config router policy ... 560
config router policy6 ... 563
config router static6 ... 564
config router ospf ... 566
config router ospf6 ... 580
config router bgp ... 593
config router isis ... 630
config router multicast-flow ... 643
config router multicast ... 644
config router multicast6 ... 652
config router info ... 653

config router info6 ... 654
config router auth-path ... 654
config router setting ... 654
config router bfd ... 655
config router bfd6 ... 655
ssh-filter ... 656
config ssh-filter profile ... 656
switch-controller ... 661
config switch-controller traffic-policy ... 662
config switch-controller switch-interface-tag ... 663
config switch-controller 802-1X-settings ... 663
config switch-controller security-policy 802-1X ... 664
config switch-controller security-policy local-access ... 666
config switch-controller location ... 667
config switch-controller lldp-settings ... 671
config switch-controller lldp-profile ... 672
config switch-controller qos dot1p-map ... 675
config switch-controller qos ip-dscp-map ... 679
config switch-controller qos queue-policy ... 680
config switch-controller qos qos-policy ... 682
config switch-controller storm-control-policy ... 683
config switch-controller auto-config policy ... 684
config switch-controller auto-config default ... 685
config switch-controller auto-config custom ... 686
config switch-controller switch-profile ... 686
config switch-controller custom-command ... 687
config switch-controller virtual-port-pool ... 687
config switch-controller managed-switch ... 688
config switch-controller switch-group ... 715
config switch-controller stp-settings ... 715
config switch-controller stp-instance ... 716
config switch-controller storm-control ... 717
config switch-controller global ... 718
config switch-controller system ... 720
config switch-controller poe ... 721
config switch-controller switch-log ... 721
config switch-controller igmp-snooping ... 722
config switch-controller sflow ... 723
config switch-controller quarantine ... 723
config switch-controller network-monitor-settings ... 724
config switch-controller flow-tracking ... 725
config switch-controller snmp-sysinfo ... 727
config switch-controller snmp-trap-threshold ... 728
config switch-controller snmp-community ... 729
config switch-controller snmp-user ... 731
config switch-controller traffic-sniffer ... 732
config switch-controller remote-log ... 734
system ... 737
config system vdom ... 740

config system global ... 741
config system accprofile ... 774
config system npu ... 783
config system vdom-link ... 788
config system switch-interface ... 789
config system object-tagging ... 790
config system lte-modem ... 792
config system interface ... 793
config system physical-switch ... 833
config system virtual-switch ... 834
config system stp ... 836
config system password-policy ... 837
config system password-policy-guest-admin ... 840
config system sms-server ... 842
config system custom-language ... 842
config system admin ... 842
config system api-user ... 849
config system sso-admin ... 850
config system settings ... 850
config system sit-tunnel ... 870
config system fsso-polling ... 871
config system ha ... 872
config system ha-monitor ... 882
config system storage ... 883
config system dedicated-mgmt ... 884
config system arp-table ... 885
config system ipv6-neighbor-cache ... 886
config system dns ... 886
config system ddns ... 888
config system sflow ... 890
config system vdom-sflow ... 891
config system netflow ... 892
config system vdom-netflow ... 892
config system vdom-dns ... 893
config system replacemsg-image ... 895
config system replacemsg mail ... 895
config system replacemsg http ... 896
config system replacemsg webproxy ... 897
config system replacemsg ftp ... 898
config system replacemsg nntp ... 898
config system replacemsg fortiguard-wf ... 899
config system replacemsg spam ... 900
config system replacemsg alertmail ... 901
config system replacemsg admin ... 902
config system replacemsg auth ... 902
config system replacemsg sslvpn ... 903
config system replacemsg device-detection-portal ... 904
config system replacemsg nac-quar ... 905
config system replacemsg traffic-quota ... 906

config system replacemsg utm ... 906
config system replacemsg icap ... 907
config system replacemsg-group ... 908
config system snmp sysinfo ... 920
config system snmp community ... 921
config system snmp user ... 925
config system autoupdate push-update ... 929
config system autoupdate schedule ... 930
config system autoupdate tunneling ... 931
config system session-ttl ... 932
config system dhcp server ... 933
config system dhcp6 server ... 944
config system modem ... 946
config system 3g-modem custom ... 953
config system status ... 954
config system performance status ... 954
config system performance top ... 954
config system performance firewall packet-distribution ... 955
config system performance firewall statistics ... 955
config system session ... 955
config system session6 ... 955
config system cmdb ... 955
config system fortiguard-service ... 956
config system fortianalyzer-connectivity ... 956
config system checksum status ... 956
config system mgmt-csum ... 956
config system ha-nonsync-csum ... 956
config system fortiguard-log-service ... 956
config system central-mgmt ... 957
config system alias ... 957
config system auto-script ... 957
config system info admin status ... 958
config system info admin ssh ... 958
config system management-tunnel ... 958
config system fortimanager ... 960
config system fm ... 961
config system central-management ... 962
config system zone ... 966
config system geoip-country ... 967
config system sdn-connector ... 968
config system ipv6-tunnel ... 973
config system external-resource ... 974
config system ips-urlfilter-dns ... 975
config system ips-urlfilter-dns6 ... 976
config system network-visibility ... 976
config system gre-tunnel ... 977
config system ipsec-aggregate ... 979
config system ipip-tunnel ... 979
config system mobile-tunnel ... 980

config system pppoe-interface 982
config system vxlan 984
config system geneve 985
config system virtual-wire-pair 986
config system dns-database 987
config system dns-server 990
config system resource-limits 990
config system vdom-property 993
config system virtual-wan-link 995
config system speed-test-server 1010
config system lldp network-policy 1011
config system cluster-sync 1018
config system fortiguard 1021
config system arp 1027
config system email-server 1027
config system alarm 1028
config system mac-address-table 1031
config system session-helper 1032
config system proxy-arp 1033
config system fips-cc 1033
config system tos-based-priority 1034
config system dscp-based-priority 1035
config system probe-response 1036
config system link-monitor 1037
config system auto-install 1040
config system console 1041
config system ntp 1042
config system ptp 1045
config system wccp 1046
config system nat64 1049
config system vdom-radius-server 1051
config system startup-error-log 1051
config system source-ip status 1051
config system auto-update status 1052
config system auto-update versions 1052
config system session-info list 1052
config system session-info expectation 1052
config system session-info full-stat 1052
config system session-info statistics 1052
config system session-info ttl 1053
config system session-helper-info list 1053
config system ip-conflict status 1053
config system ftm-push 1053
config system geoip-override 1054
config system fortisandbox 1055
config system vdom-exception 1056
config system csf 1057
config system automation-trigger 1059
config system automation-action 1062

config system automation-destination ... 1067
config system automation-stitch ... 1068
config system nd-proxy ... 1069
config system saml ... 1069
test ... 1073
config test smtp ... 1074
config test ftpd ... 1074
config test pop3 ... 1075
config test imap ... 1075
config test nntp ... 1075
config test harelay ... 1076
config test hasync ... 1076
config test hatalk ... 1076
config test sessionsync ... 1077
config test forticldd ... 1077
config test miglogd ... 1077
config test urlfilter ... 1078
config test wf_monitor ... 1078
config test ovrd ... 1078
config test ipsmonitor ... 1079
config test ipsengine ... 1079
config test ipldbd ... 1079
config test ddnscd ... 1080
config test snmpd ... 1080
config test acd ... 1080
config test dnsproxy ... 1081
config test sflowd ... 1081
config test init ... 1081
config test l2tpcd ... 1082
config test dhcprelay ... 1082
config test pptpcd ... 1082
config test wccpd ... 1083
config test wad ... 1083
config test radiusd ... 1083
config test fsd ... 1084
config test ipsufd ... 1084
config test lted ... 1084
config test forticron ... 1085
config test uploadd ... 1085
config test quarantined ... 1086
config test dhcp6c ... 1086
config test info-sslvpnd ... 1086
config test dsd ... 1087
config test ipmc_sensord ... 1087
config test lnkmtd ... 1087
config test dhcp6r ... 1088
config test awsd ... 1088
config test netxd ... 1088
config test fnbamd ... 1089

config test mrd 1089
config test zebos_launcher 1089
config test radius-das 1090
config test csfd 1090
config test fsvrd 1090
config test radvd 1091
config test fcnacd 1091
config test sdncd 1091
config test azd 1092
config test gcpd 1092
config test ocid 1092
config test kubed 1093
config test autod 1093
config test bfd 1093
config test openstackd 1094
config test vmwd 1094
config test fas 1094
config test sepmd 1095
user 1096
config user radius 1096
config user tacacs+ 1106
config user exchange 1108
config user ldap 1110
config user krb-keytab 1114
config user domain-controller 1115
config user pop3 1116
config user saml 1117
config user fsso 1118
config user adgrp 1121
config user fsso-polling 1122
config user fortitoken 1123
config user password-policy 1124
config user local 1125
config user setting 1128
config user peer 1132
config user peergrp 1134
config user quarantine 1134
config user group 1135
config user security-exempt-list 1140
voip 1142
config voip profile 1142
vpn 1162
config vpn certificate ca 1162
config vpn certificate remote 1164
config vpn certificate local 1165
config vpn certificate crl 1167
config vpn certificate ocsp-server 1169
config vpn certificate setting 1170
config vpn ssl web realm 1173

config vpn ssl web host-check-software 1174
config vpn ssl web portal 1175
config vpn ssl web user-group-bookmark 1190
config vpn ssl web user-bookmark 1194
config vpn ssl settings 1198
config vpn ssl monitor 1209
config vpn ipsec phase1 1210
config vpn ipsec phase2 1227
config vpn ipsec manualkey 1234
config vpn ipsec concentrator 1236
config vpn ipsec phase1-interface 1236
config vpn ipsec phase2-interface 1258
config vpn ipsec manualkey-interface 1266
config vpn ipsec forticlient 1268
config vpn ipsec stats crypto 1269
config vpn ipsec stats tunnel 1269
config vpn ipsec tunnel details 1269
config vpn ipsec tunnel summary 1269
config vpn ipsec tunnel name 1269
config vpn pptp 1270
config vpn l2tp 1270
config vpn ocvpn 1271
config vpn ike gateway 1274
config vpn status l2tp 1274
config vpn status pptp 1274
config vpn status ssl list 1274
config vpn status ssl hw-acceleration-status 1275
waf 1276
config waf main-class 1276
config waf sub-class 1276
config waf signature 1277
config waf profile 1277
web-proxy 1303
config web-proxy profile 1303
config web-proxy global 1307
config web-proxy explicit 1309
config web-proxy forward-server 1314
config web-proxy forward-server-group 1315
config web-proxy debug-url 1317
config web-proxy wisp 1318
config web-proxy url-match 1318
webfilter 1320
config webfilter ftgd-local-cat 1320
config webfilter content 1321
config webfilter content-header 1322
config webfilter urlfilter 1323
config webfilter ips-urlfilter-setting 1326
config webfilter ips-urlfilter-setting6 1326
config webfilter ips-urlfilter-cache-setting 1327

config webfilter profile ... 1327
config webfilter fortiguard ... 1343
config webfilter categories ... 1345
config webfilter override ... 1345
config webfilter ftgd-local-rating ... 1346
config webfilter search-engine ... 1347
config webfilter ftgd-statistics ... 1348
config webfilter status ... 1348
config webfilter override-usr ... 1348
wireless-controller ... 1349
config wireless-controller inter-controller ... 1350
config wireless-controller global ... 1351
config wireless-controller hotspot20 anqp-venue-name ... 1354
config wireless-controller hotspot20 anqp-network-auth-type ... 1354
config wireless-controller hotspot20 anqp-roaming-consortium ... 1355
config wireless-controller hotspot20 anqp-nai-realm ... 1356
config wireless-controller hotspot20 anqp-3gpp-cellular ... 1359
config wireless-controller hotspot20 anqp-ip-address-type ... 1359
config wireless-controller hotspot20 h2qp-operator-name ... 1360
config wireless-controller hotspot20 h2qp-wan-metric ... 1361
config wireless-controller hotspot20 h2qp-conn-capability ... 1362
config wireless-controller hotspot20 icon ... 1365
config wireless-controller hotspot20 h2qp-osu-provider ... 1366
config wireless-controller hotspot20 qos-map ... 1367
config wireless-controller hotspot20 hs-profile ... 1368
config wireless-controller vap ... 1375
config wireless-controller timers ... 1399
config wireless-controller setting ... 1400
config wireless-controller log ... 1407
config wireless-controller bonjour-profile ... 1412
config wireless-controller region ... 1413
config wireless-controller vap-group ... 1414
config wireless-controller wids-profile ... 1414
config wireless-controller ble-profile ... 1421
config wireless-controller wtp-profile ... 1423
config wireless-controller wtp ... 1475
config wireless-controller wtp-group ... 1496
config wireless-controller qos-profile ... 1498
config wireless-controller wag-profile ... 1502
config wireless-controller utm-profile ... 1503
config wireless-controller address ... 1504
config wireless-controller addrgrp ... 1505
config wireless-controller snmp ... 1505
config wireless-controller scan ... 1509
config wireless-controller ap-status ... 1509
config wireless-controller wlchanlistlic ... 1510
config wireless-controller status ... 1510
config wireless-controller wtp-status ... 1510
config wireless-controller client-info ... 1510

config wireless-controller vap-status 1511
config wireless-controller rf-analysis 1511
config wireless-controller spectral-info 1511

Change Log

Date	Change Description
2021-06-02	First automated release of the FortiOS 6.2.9 CLI Reference.
2021-07-19	Updated config system global on page 741 to remove 3DES from strong-crypto. Updated config user fsso on page 1118 to add the collector agent maximum password length. Updated config system global on page 741 to add additional information for dnsproxy-worker-count and cloud-communication. Updated config system resource-limits on page 990 to add additional information for log-disk-quota.

FortiOS CLI reference

This document describes FortiOS 6.2.9 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI).

The CLI syntax is created by processing the schema from a FortiGate 3000D running FortiOS 6.2.9, and reformatting the resulting CLI output.

For information on using the CLI, see the FortiOS 6.2.9 Cookbook, 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.

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, low-end FortiGate models do not support the aggregate interface type option of the `config system interface` command.

Hardware configuration

For example, some AMC module commands are only available when an AMC module is installed.

FortiOS Carrier, FortiGate Voice, FortiWiFi, 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 CLI syntax is created by processing the schema from a FortiGate 3000D running FortiOS6.2.9, and reformatting the resulting CLI output.

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 20

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
username	Name that appears in the From: field of alert emails (max. 36 characters).	string	Maximum length: 63
mailto1	Email address to send alert email to (usually a system administrator) (max. 64 characters).	string	Maximum length: 63
mailto2	Optional second email address to send alert email to (max. 64 characters).	string	Maximum length: 63
mailto3	Optional third email address to send alert email to (max. 64 characters).	string	Maximum length: 63
filter-mode	How to filter log messages that are sent to alert emails.	option	-

Option	Description
category	Filter based on category.
threshold	Filter based on severity.

Parameter	Description	Type	Size
email-interval	Interval between sending alert emails .	integer	Minimum value: 1 Maximum value: 99999
IPS-logs	Enable/disable IPS logs in alert email.	option	-

Option	Description
enable	Enable IPS logs in alert email.
disable	Disable IPS logs in alert email.

Parameter	Description	Type	Size
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-

Option	Description
enable	Enable firewall authentication failure logs in alert email.
disable	Disable firewall authentication failure logs in alert email.

Parameter	Description	Type	Size
HA-logs	Enable/disable HA logs in alert email.	option	-

Option	Description
enable	Enable HA logs in alert email.
disable	Disable HA logs in alert email.

Parameter	Description	Type	Size
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-

Option	Description
enable	Enable IPsec error logs in alert email.
disable	Disable IPsec error logs in alert email.

Parameter	Description	Type	Size
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-

Option	Description
enable	Enable FortiGuard update logs in alert email.
disable	Disable FortiGuard update logs in alert email.

Parameter	Description	Type	Size
PPP-errors-logs	Enable/disable PPP error logs in alert email.	option	-

Option	Description
enable	Enable PPP error logs in alert email.
disable	Disable PPP error logs in alert email.

Parameter	Description	Type	Size
sslvpn-authentication-errors-logs	Enable/disable SSL-VPN authentication error logs in alert email.	option	-

Option	Description
enable	Enable SSL-VPN authentication error logs in alert email.
disable	Disable SSL-VPN authentication error logs in alert email.

Parameter	Description	Type	Size
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-

Option	Description
enable	Enable antivirus logs in alert email.
disable	Disable antivirus logs in alert email.

Parameter	Description	Type	Size
webfilter-logs	Enable/disable web filter logs in alert email.	option	-

Option	Description
enable	Enable web filter logs in alert email.
disable	Disable web filter logs in alert email.

Parameter	Description	Type	Size
configuration-changes-logs	Enable/disable configuration change logs in alert email.	option	-

Parameter	Description	Type	Size
	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	-
	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	-
	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	-
	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	-
	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	-
	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	-

Parameter	Description	Type	Size
	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	-
	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	-
	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	-
	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
local-disk-usage	Disk usage percentage at which to send alert email .	integer	Minimum value: 1 Maximum value: 99
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999

Parameter	Description	Type	Size
alert-interval	Alert alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
critical-interval	Critical alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
error-interval	Error alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
debug-interval	Debug alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999
severity	Lowest severity level to log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

antivirus

This section includes syntax for the following commands:

- config antivirus heuristic on page 27
- config antivirus profile on page 32
- config antivirus quarantine on page 27
- config antivirus settings on page 26

config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
   Description: Configure AntiVirus settings.
   set default-db [normal|extended]
   set grayware [enable|disable]
   set override-timeout {integer}
end
```

config antivirus settings

Parameter	Description	Type	Size
default-db	Select the AV database to be used for AV scanning.	option	-

Option	Description
normal	Use the normal AntiVirus database.
extended	Use the extended AntiVirus database.

Parameter	Description	Type	Size
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-

Option	Description
enable	Enable grayware detection.
disable	Disable grayware detection.

Parameter	Description	Type	Size
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

config antivirus heuristic

Configure global heuristic options.

```
config antivirus heuristic
   Description: Configure global heuristic options.
   set mode [pass|block|...]
end
```

config antivirus heuristic

Parameter	Description	Type	Size
mode	Enable/disable heuristics and determine how the system behaves if heuristics detects a problem.	option	-

Option	Description
pass	Enable heuristics but detected files are passed. If enabled, the system will record a log message.
block	Enable heuristics and detected files are blocked. If enabled, the system will record a log message.
disable	Turn off heuristics.

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-heuristic {option1}, {option2}, ...
   set store-heuristic {option1}, {option2}, ...
   set lowspace [drop-new|ovrw-old]
   set destination [NULL|disk|...]
end
```

config antivirus quarantine

Parameter	Description	Type	Size
agelimit	Age limit for quarantined files .	integer	Minimum value: 0 Maximum value: 479
maxfilesize	Maximum file size to quarantine .	integer	Minimum value: 0 Maximum value: 500
quarantine-quota	The amount of disk space to reserve for quarantining files .	integer	Minimum value: 0 Maximum value: 4294967295
drop-infected	Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-

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

store-infected	Quarantine infected files found in sessions using the selected protocols.	option	-

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

Parameter	Description	Type	Size
	Option / **Description** *cifs* — CIFS. *ssh* — SSH.		
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-
	Option / **Description** *imap* — IMAP. *smtp* — SMTP. *pop3* — POP3. *http* — HTTP. *ftp* — FTP. *nntp* — NNTP. *imaps* — IMAPS. *smtps* — SMTPS. *pop3s* — POP3S. *ftps* — FTPS. *mapi* — MAPI. *cifs* — CIFS. *ssh* — SSH.		
drop-heuristic	Do not quarantine files detected by heuristics found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-
	Option / **Description** *imap* — IMAP. *smtp* — SMTP. *pop3* — POP3. *http* — HTTP. *ftp* — FTP. *nntp* — NNTP. *imaps* — IMAPS.		

Parameter	Description	Type	Size

Option	Description
smtps	SMTPS.
pop3s	POP3S.
https	HTTPS.
ftps	FTPS.
mapi	MAPI.
cifs	CIFS.
ssh	SSH.

store-heuristic	Quarantine files detected by heuristics found in sessions using the selected protocols.	option	-

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

lowspace	Select the method for handling additional files when running low on disk space.	option	-

Option	Description
drop-new	Drop (delete) the most recently quarantined files.

Parameter	Description	Type	Size
	Option / **Description** *ovrw-old* / 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	-
	Option / **Description** *NULL* / Files that would be quarantined are deleted. *disk* / Quarantine files to the FortiGate hard disk. *FortiAnalyzer* / FortiAnalyzer		

config antivirus profile

Configure AntiVirus profiles.

```
config antivirus profile
   Description: Configure AntiVirus profiles.
   edit <name>
      set comment {var-string}
      set replacemsg-group {string}
      set ftgd-analytics [disable|suspicious|...]
      set analytics-max-upload {integer}
      set analytics-wl-filetype {integer}
      set analytics-bl-filetype {integer}
      set analytics-db [disable|enable]
      set mobile-malware-db [disable|enable]
      config http
         Description: Configure HTTP AntiVirus options.
         set options {option1}, {option2}, ...
         set archive-block {option1}, {option2}, ...
         set archive-log {option1}, {option2}, ...
         set emulator [enable|disable]
         set outbreak-prevention [disabled|files|...]
         set content-disarm [disable|enable]
      end
      config ftp
         Description: Configure FTP AntiVirus options.
         set options {option1}, {option2}, ...
         set archive-block {option1}, {option2}, ...
         set archive-log {option1}, {option2}, ...
         set emulator [enable|disable]
         set outbreak-prevention [disabled|files|...]
      end
      config imap
         Description: Configure IMAP AntiVirus options.
         set options {option1}, {option2}, ...
         set archive-block {option1}, {option2}, ...
```

```
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set outbreak-prevention [disabled|files|...]
    set content-disarm [disable|enable]
end
config pop3
    Description: Configure POP3 AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set outbreak-prevention [disabled|files|...]
    set content-disarm [disable|enable]
end
config smtp
    Description: Configure SMTP AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set outbreak-prevention [disabled|files|...]
    set content-disarm [disable|enable]
end
config mapi
    Description: Configure MAPI AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set outbreak-prevention [disabled|files|...]
end
config nntp
    Description: Configure NNTP AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set outbreak-prevention [disabled|files|...]
end
config cifs
    Description: Configure CIFS AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set outbreak-prevention [disabled|files|...]
end
config ssh
    Description: Configure SFTP and SCP AntiVirus options.
    set options {option1}, {option2}, ...
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
```

```
        set outbreak-prevention [disabled|files|...]
    end
    config nac-quar
        Description: Configure AntiVirus quarantine settings.
        set infected [none|quar-src-ip]
        set expiry {user}
        set log [enable|disable]
    end
    config outbreak-prevention
        Description: Configure Virus Outbreak Prevention settings.
        set ftgd-service [disable|enable]
        set external-blocklist [disable|enable]
    end
    config content-disarm
        Description: AV Content Disarm and Reconstruction settings.
        set original-file-destination [fortisandbox|quarantine|...]
        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 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
comment	Comment.	var-string	Maximum length: 255
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Do not upload files to FortiSandbox. *suspicious* — Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious. *everything* — Submit all files scanned by AntiVirus to FortiSandbox. AntiVirus may not scan all files.		
analytics-max-upload	Maximum size of files that can be uploaded to FortiSandbox .	integer	Minimum value: 1 Maximum value: 186 **
analytics-wl-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295
analytics-bl-filetype	Only submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295
analytics-db	Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.	option	-
	Option / **Description** *disable* — Use only the standard AV signature databases. *enable* — Also use the FortiSandbox signature database.		
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-
	Option / **Description** *disable* — Do not use the mobile malware signature database. *enable* — Also use the mobile malware signature database.		
av-virus-log	Enable/disable AntiVirus logging.	option	-
	Option / **Description** *enable* — Enable setting.		

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable setting.		
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
extended-log	Enable/disable extended logging for antivirus.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
scan-mode	Choose between default scan mode and legacy scan mode.	option	-
	Option / **Description** *default* / Aggregate scanning mode. *legacy* / Force scanunit to scan all files.		

** Values may differ between models.

config http

Parameter	Description	Type	Size
options	Enable/disable HTTP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option / **Description** *scan* / Enable HTTP antivirus scanning. *avmonitor* / Enable HTTP antivirus logging. *quarantine* / Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-
	Option / **Description** *encrypted* / Block encrypted archives.		

Parameter	Description	Type	Size
	Option / **Description** *corrupted* / Block corrupted archives. *partiallycorrupted* / Block partially corrupted archives. *multipart* / Block multipart archives. *nested* / Block nested archives. *mailbomb* / Block mail bomb archives. *fileslimit* / Block exceeded archive files limit. *timeout* / Block scan timeout. *unhandled* / Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-
	Option / **Description** *encrypted* / Log encrypted archives. *corrupted* / Log corrupted archives. *partiallycorrupted* / Log partially corrupted archives. *multipart* / Log multipart archives. *nested* / Log nested archives. *mailbomb* / Log mail bomb archives. *fileslimit* / Log exceeded archive files limit. *timeout* / Log scan timeout. *unhandled* / Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option / **Description** *enable* / Enable the virus emulator. *disable* / Disable the virus emulator.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option / **Description** *disabled* / Disabled. *files* / Analyze files as sent, not the content of archives.		

Parameter	Description	Type	Size
	Option **Description** *full-archive* Analyze files including the content of archives.		
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-
	Option **Description** *disable* Disable Content Disarm and Reconstruction for this protocol. *enable* Enable Content Disarm and Reconstruction for this protocol.		

config ftp

Parameter	Description	Type	Size
options	Enable/disable FTP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option **Description** *scan* Enable FTP antivirus scanning. *avmonitor* Enable FTP antivirus logging. *quarantine* Enable FTP antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives. *nested* Block nested archives. *mailbomb* Block mail bomb archives. *fileslimit* Block exceeded archive files limit. *timeout* Block scan timeout. *unhandled* Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-

Parameter	Description	Type	Size
	Option **Description** *encrypted* Log encrypted archives. *corrupted* Log corrupted archives. *partiallycorrupted* Log partially corrupted archives. *multipart* Log multipart archives. *nested* Log nested archives. *mailbomb* Log mail bomb archives. *fileslimit* Log exceeded archive files limit. *timeout* Log scan timeout. *unhandled* Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option **Description** *disabled* Disabled. *files* Analyze files as sent, not the content of archives. *full-archive* Analyze files including the content of archives.		

config imap

Parameter	Description	Type	Size
options	Enable/disable IMAP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option **Description** *scan* Enable IMAP antivirus scanning. *avmonitor* Enable IMAP antivirus logging. *quarantine* Enable IMAP antivirus quarantine. Files are quarantined depending on quarantine settings.		

Parameter	Description	Type	Size
archive-block	Select the archive types to block.	option	-

Option	Description
encrypted	Block encrypted archives.
corrupted	Block corrupted archives.
partiallycorrupted	Block partially corrupted archives.
multipart	Block multipart archives.
nested	Block nested archives.
mailbomb	Block mail bomb archives.
fileslimit	Block exceeded archive files limit.
timeout	Block scan timeout.
unhandled	Block archives that FortiOS cannot open.

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

Option	Description
encrypted	Log encrypted archives.
corrupted	Log corrupted archives.
partiallycorrupted	Log partially corrupted archives.
multipart	Log multipart archives.
nested	Log nested archives.
mailbomb	Log mail bomb archives.
fileslimit	Log exceeded archive files limit.
timeout	Log scan timeout.
unhandled	Log archives that FortiOS cannot open.

emulator	Enable/disable the virus emulator.	option	-

Option	Description
enable	Enable the virus emulator.
disable	Disable the virus emulator.

executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-

Parameter	Description	Type	Size
	Option **Description** *default* Perform standard AntiVirus scanning of Windows executable files. *virus* Treat Windows executables as viruses.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option **Description** *disabled* Disabled. *files* Analyze files as sent, not the content of archives. *full-archive* Analyze files including the content of archives.		
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-
	Option **Description** *disable* Disable Content Disarm and Reconstruction for this protocol. *enable* Enable Content Disarm and Reconstruction for this protocol.		

config pop3

Parameter	Description	Type	Size
options	Enable/disable POP3 AntiVirus scanning, monitoring, and quarantine.	option	-
	Option **Description** *scan* Enable POP3 antivirus scanning. *avmonitor* Enable POP3 antivirus logging. *quarantine* Enable POP3 antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives.		

Parameter	Description	Type	Size
	Option / **Description** *multipart* — Block multipart archives. *nested* — Block nested archives. *mailbomb* — Block mail bomb archives. *fileslimit* — Block exceeded archive files limit. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives. *mailbomb* — Log mail bomb archives. *fileslimit* — Log exceeded archive files limit. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-
	Option / **Description** *default* — Perform standard AntiVirus scanning of Windows executable files. *virus* — Treat Windows executables as viruses.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disabled* — Disabled. *files* — Analyze files as sent, not the content of archives. *full-archive* — Analyze files including the content of archives.		
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-
	Option / **Description** *disable* — Disable Content Disarm and Reconstruction for this protocol. *enable* — Enable Content Disarm and Reconstruction for this protocol.		

config smtp

Parameter	Description	Type	Size
options	Enable/disable SMTP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option / **Description** *scan* — Enable SMTP antivirus scanning. *avmonitor* — Enable SMTP antivirus logging. *quarantine* — Enable SMTP antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-
	Option / **Description** *encrypted* — Block encrypted archives. *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives. *mailbomb* — Block mail bomb archives. *fileslimit* — Block exceeded archive files limit. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiOS cannot open.		

Parameter	Description	Type	Size
archive-log	Select the archive types to log.	option	-

Option	Description
encrypted	Log encrypted archives.
corrupted	Log corrupted archives.
partiallycorrupted	Log partially corrupted archives.
multipart	Log multipart archives.
nested	Log nested archives.
mailbomb	Log mail bomb archives.
fileslimit	Log exceeded archive files limit.
timeout	Log scan timeout.
unhandled	Log archives that FortiOS cannot open.

emulator	Enable/disable the virus emulator.	option	-

Option	Description
enable	Enable the virus emulator.
disable	Disable the virus emulator.

executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-

Option	Description
default	Perform standard AntiVirus scanning of Windows executable files.
virus	Treat Windows executables as viruses.

outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-

Option	Description
disabled	Disabled.
files	Analyze files as sent, not the content of archives.
full-archive	Analyze files including the content of archives.

content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable Content Disarm and Reconstruction for this protocol. *enable* Enable Content Disarm and Reconstruction for this protocol.		

config mapi

Parameter	Description	Type	Size
options	Enable/disable MAPI AntiVirus scanning, monitoring, and quarantine.	option	-
	Option **Description** *scan* Enable MAPI antivirus scanning. *avmonitor* Enable MAPI antivirus logging. *quarantine* Enable MAPI antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives. *nested* Block nested archives. *mailbomb* Block mail bomb archives. *fileslimit* Block exceeded archive files limit. *timeout* Block scan timeout. *unhandled* Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-
	Option **Description** *encrypted* Log encrypted archives. *corrupted* Log corrupted archives. *partiallycorrupted* Log partially corrupted archives.		

Parameter	Description	Type	Size
	Option / **Description** *multipart* / Log multipart archives. *nested* / Log nested archives. *mailbomb* / Log mail bomb archives. *fileslimit* / Log exceeded archive files limit. *timeout* / Log scan timeout. *unhandled* / Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option / **Description** *enable* / Enable the virus emulator. *disable* / Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-
	Option / **Description** *default* / Perform standard AntiVirus scanning of Windows executable files. *virus* / Treat Windows executables as viruses.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option / **Description** *disabled* / Disabled. *files* / Analyze files as sent, not the content of archives. *full-archive* / Analyze files including the content of archives.		

config nntp

Parameter	Description	Type	Size
options	Enable/disable NNTP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option / **Description** *scan* / Enable NNTP antivirus scanning. *avmonitor* / Enable NNTP antivirus logging.		

Parameter	Description	Type	Size
	Option / **Description** *quarantine* / Enable NNTP antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-
	Option / **Description** *encrypted* / Block encrypted archives. *corrupted* / Block corrupted archives. *partiallycorrupted* / Block partially corrupted archives. *multipart* / Block multipart archives. *nested* / Block nested archives. *mailbomb* / Block mail bomb archives. *fileslimit* / Block exceeded archive files limit. *timeout* / Block scan timeout. *unhandled* / Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-
	Option / **Description** *encrypted* / Log encrypted archives. *corrupted* / Log corrupted archives. *partiallycorrupted* / Log partially corrupted archives. *multipart* / Log multipart archives. *nested* / Log nested archives. *mailbomb* / Log mail bomb archives. *fileslimit* / Log exceeded archive files limit. *timeout* / Log scan timeout. *unhandled* / Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option / **Description** *enable* / Enable the virus emulator. *disable* / Disable the virus emulator.		

Parameter	Description	Type	Size
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-

Option	Description
disabled	Disabled.
files	Analyze files as sent, not the content of archives.
full-archive	Analyze files including the content of archives.

config cifs

Parameter	Description	Type	Size
options	Enable/disable CIFS AntiVirus scanning, monitoring, and quarantine.	option	-

Option	Description
scan	Enable CIFS antivirus scanning.
avmonitor	Enable CIFS antivirus logging.
quarantine	Enable CIFS antivirus quarantine. Files are quarantined depending on quarantine settings.

Parameter	Description	Type	Size
archive-block	Select the archive types to block.	option	-

Option	Description
encrypted	Block encrypted archives.
corrupted	Block corrupted archives.
partiallycorrupted	Block partially corrupted archives.
multipart	Block multipart archives.
nested	Block nested archives.
mailbomb	Block mail bomb archives.
fileslimit	Block exceeded archive files limit.
timeout	Block scan timeout.
unhandled	Block archives that FortiOS cannot open.

Parameter	Description	Type	Size
archive-log	Select the archive types to log.	option	-

Option	Description
encrypted	Log encrypted archives.

Parameter	Description	Type	Size
	Option **Description** *corrupted* Log corrupted archives. *partiallycorrupted* Log partially corrupted archives. *multipart* Log multipart archives. *nested* Log nested archives. *mailbomb* Log mail bomb archives. *fileslimit* Log exceeded archive files limit. *timeout* Log scan timeout. *unhandled* Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option **Description** *disabled* Disabled. *files* Analyze files as sent, not the content of archives. *full-archive* Analyze files including the content of archives.		

config ssh

Parameter	Description	Type	Size
options	Enable/disable SFTP and SCP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option **Description** *scan* Enable SSH antivirus scanning. *avmonitor* Enable SSH antivirus logging. *quarantine* Enable SSH antivirus quarantine. Files are quarantined depending on quarantine settings.		
archive-block	Select the archive types to block.	option	-

Parameter	Description	Type	Size
	Option / **Description** *encrypted* / Block encrypted archives. *corrupted* / Block corrupted archives. *partiallycorrupted* / Block partially corrupted archives. *multipart* / Block multipart archives. *nested* / Block nested archives. *mailbomb* / Block mail bomb archives. *fileslimit* / Block exceeded archive files limit. *timeout* / Block scan timeout. *unhandled* / Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-
	Option / **Description** *encrypted* / Log encrypted archives. *corrupted* / Log corrupted archives. *partiallycorrupted* / Log partially corrupted archives. *multipart* / Log multipart archives. *nested* / Log nested archives. *mailbomb* / Log mail bomb archives. *fileslimit* / Log exceeded archive files limit. *timeout* / Log scan timeout. *unhandled* / Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-
	Option / **Description** *enable* / Enable the virus emulator. *disable* / Disable the virus emulator.		
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option / **Description** *disabled* / Disabled.		

Parameter	Description	Type	Size

Option	Description
files	Analyze files as sent, not the content of archives.
full-archive	Analyze files including the content of archives.

config nac-quar

Parameter	Description	Type	Size
infected	Enable/Disable quarantining infected hosts to the banned user list.	option	-

Option	Description
none	Do not quarantine infected hosts.
quar-src-ip	Quarantine all traffic from the infected hosts source IP.

expiry	Duration of quarantine.	user	Not Specified
log	Enable/disable AntiVirus quarantine logging.	option	-

Option	Description
enable	Enable AntiVirus quarantine logging.
disable	Disable AntiVirus quarantine logging.

config outbreak-prevention

Parameter	Description	Type	Size
ftgd-service	Enable/disable FortiGuard Virus outbreak prevention service.	option	-

Option	Description
disable	Disable FortiGuard Virus Outbreak Prevention service.
enable	Enable FortiGuard Virus Outbreak Prevention service.

external-blocklist	Enable/disable external malware blocklist.	option	-

Option	Description
disable	Disable external malware blocklist.
enable	Enable external malware blocklist.

config content-disarm

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

Option	Description
fortisandbox	Send original file to configured FortiSandbox.
quarantine	Send original file to quarantine.
discard	Original file will be discarded after content disarm.

Parameter	Description	Type	Size
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-

Option	Description
disable	Disable this Content Disarm and Reconstruction feature.
enable	Enable this Content Disarm and Reconstruction feature.

Parameter	Description	Type	Size
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-

Option	Description
disable	Disable this Content Disarm and Reconstruction feature.
enable	Enable this Content Disarm and Reconstruction feature.

Parameter	Description	Type	Size
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-

Option	Description
disable	Disable this Content Disarm and Reconstruction feature.
enable	Enable this Content Disarm and Reconstruction feature.

Parameter	Description	Type	Size
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-

Option	Description
disable	Disable this Content Disarm and Reconstruction feature.
enable	Enable this Content Disarm and Reconstruction feature.

Parameter	Description	Type	Size
office-dde	Enable/disable stripping of Dynamic Data Exchange events in Microsoft Office documents.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-
	Option **Description** *disable* Disable this Content Disarm and Reconstruction feature. *enable* Enable this Content Disarm and Reconstruction feature.		
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-

Parameter	Description	Type	Size

Option	Description
disable	Disable this Content Disarm and Reconstruction feature.
enable	Enable this Content Disarm and Reconstruction feature.

application

This section includes syntax for the following commands:

- config application rule-settings on page 58
- config application group on page 66
- config application list on page 59
- config application name on page 56
- config application custom on page 58

config application name

Configure application signatures.

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

config application name

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

Parameter	Description	Type	Size
category	Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295
sub-category	Application sub-category ID.	integer	Minimum value: 0 Maximum value: 255
popularity	Application popularity.	integer	Minimum value: 0 Maximum value: 255
risk	Application risk.	integer	Minimum value: 0 Maximum value: 255
weight	Application weight.	integer	Minimum value: 0 Maximum value: 255
protocol	Application protocol.	user	Not Specified
technology	Application technology.	user	Not Specified
behavior	Application behavior.	user	Not Specified
vendor	Application vendor.	user	Not Specified
parameter	Application parameter name.	string	Maximum length: 35

config metadata

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

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
id	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295
comment	Comment.	string	Maximum length: 63
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295
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-black-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 sub-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>
                  set value {string}
               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
comment	comments	var-string	Maximum length: 255
replacemsg-group	Replacement message group.	string	Maximum length: 35
extended-log	Enable/disable extended logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

other-application-action	Action for other applications.	option	-

Option	Description
pass	Allow sessions matching an application in this application list.
block	Block sessions matching an application in this application list.

app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-

Option	Description
disable	Disable replacement messages for blocked applications.
enable	Enable replacement messages for blocked applications.

other-application-log	Enable/disable logging for other applications.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable logging for other applications. *enable* Enable logging for other applications.		
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-
	Option **Description** *disable* Disable default application port enforcement. *enable* Enable default application port enforcement.		
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-
	Option **Description** *disable* Disable forced inclusion of signatures which normally require SSL deep inspection. *enable* Enable forced inclusion of signatures which normally require SSL deep inspection.		
unknown-application-action	Pass or block traffic from unknown applications.	option	-
	Option **Description** *pass* Pass or allow unknown applications. *block* Drop or block unknown applications.		
unknown-application-log	Enable/disable logging for unknown applications.	option	-
	Option **Description** *disable* Disable logging for unknown applications. *enable* Enable logging for unknown applications.		
p2p-black-list	P2P applications to be black listed.	option	-
	Option **Description** *skype* Skype.		

Parameter	Description	Type	Size
	Option **Description** *edonkey* Edonkey. *bittorrent* Bit torrent.		
deep-app-inspection	Enable/disable deep application inspection.	option	-
	Option **Description** *disable* Disable deep application inspection. *enable* Enable deep application inspection.		
options	Basic application protocol signatures allowed by default.	option	-
	Option **Description** *allow-dns* Allow DNS. *allow-icmp* Allow ICMP. *allow-http* Allow generic HTTP web browsing. *allow-ssl* Allow generic SSL communication. *allow-quic* Allow QUIC.		
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-
	Option **Description** *disable* Disable protocol enforcement over selected ports. *enable* Enable protocol enforcement over selected ports.		

config entries

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295
sub-category <id>	Application Sub-category ID list. Application sub-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
vendor	Application vendor filter.	user	Not Specified
technology	Application technology filter.	user	Not Specified
behavior	Application behavior filter.	user	Not Specified
popularity	Application popularity filter .	option	-

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	-

Option	Description
pass	Pass or allow matching traffic.

Parameter	Description	Type	Size
	Option / **Description** *block* — Block or drop matching traffic. *reset* — Reset sessions for matching traffic.		
log	Enable/disable logging for this application list.	option	-
	Option / **Description** *disable* — Disable logging. *enable* — Enable logging.		
log-packet	Enable/disable packet logging.	option	-
	Option / **Description** *disable* — Disable packet logging. *enable* — Enable packet logging.		
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535
rate-mode	Rate limit mode.	option	-
	Option / **Description** *periodical* — Allow configured number of packets every rate-duration. *continuous* — Block packets once the rate is reached.		
rate-track	Track the packet protocol field.	option	-
	Option / **Description** *none* — none *src-ip* — Source IP. *dest-ip* — Destination IP. *dhcp-client-mac* — DHCP client. *dns-domain* — DNS domain.		

Parameter	Description	Type	Size
session-ttl	Session TTL .	integer	Minimum value: 0 Maximum value: 4294967295
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	-

Option	Description
none	Quarantine is disabled.
attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.

quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-

Option	Description
disable	Disable quarantine logging.
enable	Enable quarantine logging.

config parameters

Parameter	Description	Type	Size
value	Parameter value.	string	Maximum length: 63

config default-network-services

Parameter	Description	Type	Size
port	Port number.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
services	Network protocols.	option	-

Option	Description
http	HTTP.
ssh	SSH.
telnet	TELNET.
ftp	FTP.
dns	DNS.
smtp	SMTP.
pop3	POP3.
imap	IMAP.
snmp	SNMP.
nntp	NNTP.
https	HTTPS.

Parameter	Description	Type	Size
violation-action	Action for protocols not white listed under selected port.	option	-

Option	Description
pass	Allow protocols not white listed under selected port.
monitor	Monitor protocols not white listed under selected port.
block	Block protocols not white listed under 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|category]
      set application <id1>, <id2>, ...
      set category <id1>, <id2>, ...
   next
end
```

config application group

Parameter	Description	Type	Size
comment	Comment	var-string	Maximum length: 255
type	Application group type.	option	-
	Option / **Description** *application* — Application ID. *category* — Application category ID.		
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295

authentication

This section includes syntax for the following commands:

- config authentication setting on page 71
- config authentication rule on page 69
- config authentication scheme on page 68

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

config authentication scheme

Parameter	Description	Type	Size
method	Authentication methods .	option	-

Option	Description
ntlm	NTLM authentication.
basic	Basic HTTP authentication.
digest	Digest HTTP authentication.
form	Form-based HTTP authentication.
negotiate	Negotiate authentication.
fsso	Fortinet Single Sign-On (FSSO) authentication.
rsso	RADIUS Single Sign-On (RSSO) authentication.
ssh-publickey	Public key based SSH authentication.

Parameter	Description	Type	Size
negotiate-ntlm	Enable/disable negotiate authentication for NTLM .	option	-

Option	Description
enable	Enable negotiate authentication for NTLM.
disable	Disable negotiate authentication for NTLM.

Parameter	Description	Type	Size
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35
domain-controller	Domain controller setting.	string	Maximum length: 35
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35
require-tfa	Enable/disable two-factor authentication .	option	-

Option	Description
enable	Enable two-factor authentication.
disable	Disable two-factor authentication.

Parameter	Description	Type	Size
fsso-guest	Enable/disable user fsso-guest authentication .	option	-

Option	Description
enable	Enable user fsso-guest authentication.
disable	Disable user fsso-guest authentication.

Parameter	Description	Type	Size
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 srcaddr <name1>, <name2>, ...
      set srcaddr6 <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
status	Enable/disable this authentication rule.	option	-

Option	Description
enable	Enable this authentication rule.
disable	Disable this authentication rule.

Parameter	Description	Type	Size
protocol	Select the protocol to use for authentication . Users connect to the FortiGate using this protocol and are asked to authenticate.	option	-

Option	Description
http	Use HTTP for authentication.
ftp	Use FTP for authentication.
socks	Use SOCKS for authentication.
ssh	Use SSH for authentication.

Parameter	Description	Type	Size
srcaddr <name>	Select an IPv4 source address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79
srcaddr6 <name>	Select an IPv6 source address. Required for web proxy authentication. Address name.	string	Maximum length: 79
ip-based	Enable/disable IP-based authentication. Once a user authenticates all traffic from the IP address the user authenticated from is allowed.	option	-

Option	Description
enable	Enable IP-based authentication.
disable	Disable IP-based authentication.

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

Parameter	Description	Type	Size
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35
web-auth-cookie	Enable/disable Web authentication cookies .	option	-

Option	Description
enable	Enable Web authentication cookie.
disable	Disable Web authentication cookie.

transaction-based	Enable/disable transaction based authentication .	option	-

Option	Description
enable	Enable transaction based authentication.
disable	Disable transaction based authentication.

web-portal	Enable/disable web portal for proxy transparent policy .	option	-

Option	Description
enable	Enable web-portal.
disable	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 captive-portal-port {integer}
   set auth-https [enable|disable]
   set captive-portal-ssl-port {integer}
end
```

config authentication setting

Parameter	Description	Type	Size
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35
captive-portal-type	Captive portal type.	option	-
	Option / **Description** *fqdn* — Use FQDN for captive portal. *ip* — Use an IP address for captive portal.		
captive-portal-ip	Captive portal IP address.	ipv4-address-any	Not Specified
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
captive-portal-port	Captive portal port number .	integer	Minimum value: 1 Maximum value: 65535
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
captive-portal-ssl-port	Captive portal SSL port number .	integer	Minimum value: 1 Maximum value: 65535

certificate

This section includes syntax for the following commands:

- config certificate remote on page 74
- config certificate crl on page 78
- config certificate local on page 75
- config certificate ca on page 73

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
ca	CA certificate as a PEM file.	user	Not Specified
range	Either global or VDOM IP address range for the CA certificate.	option	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

Parameter	Description	Type	Size
source	CA certificate source type.	option	-

Option	Description
factory	Factory installed certificate.

Parameter	Description	Type	Size
	Option: *user* — User generated certificate. Option: *bundle* — Bundle file certificate.		
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection. Option: *enable* — Trusted CA for SSL inspection. Option: *disable* — Untrusted CA for SSL inspection.	option	-
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
auto-update-days-warning	Number of days before an expiry-warning message is generated .	integer	Minimum value: 0 Maximum value: 4294967295
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified

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
remote	Remote certificate.	user	Not Specified
range	Either the global or VDOM IP address range for the remote certificate.	option	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

Parameter	Description	Type	Size
source	Remote certificate source type.	option	-

Option	Description
factory	Factory installed certificate.
user	User generated certificate.
bundle	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 [keyupate|renewal]
   next
```

```
end
```

config certificate local

Parameter	Description	Type	Size
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	-
	Option / **Description** *global* — Global range. *vdom* — VDOM IP address range.		
source	Certificate source type.	option	-
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.		
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295
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
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified

Parameter	Description	Type	Size
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	-

Option	Description
printable	Printable encoding (default).
utf8	UTF-8 encoding.

Parameter	Description	Type	Size
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified
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	-

Option	Description
asn1dn	ASN.1 distinguished name.
fqdn	Fully qualified domain name.

Parameter	Description	Type	Size
enroll-protocol	Certificate enrollment protocol.	option	-

Option	Description
none	None (default).
scep	Simple Certificate Enrollment Protocol.
cmpv2	Certificate Management Protocol Version 2.

Parameter	Description	Type	Size
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	-

Option	Description
keyupate	Key Update.
renewal	Renewal.

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
crl	Certificate Revocation List as a PEM file.	user	Not Specified
range	Either global or VDOM IP address range for the certificate.	option	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

Parameter	Description	Type	Size
source	Certificate source type.	option	-

Option	Description
factory	Factory installed certificate.
user	User generated certificate.
bundle	Bundle file certificate.

Parameter	Description	Type	Size
update-vdom	VDOM for CRL update.	string	Maximum length: 31
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35
ldap-username	LDAP server user name.	string	Maximum length: 63

Parameter	Description	Type	Size
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
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
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified

cifs

This section includes syntax for the following commands:

- config cifs profile on page 80
- config cifs domain-controller on page 80

config cifs domain-controller

Define known domain controller servers.

```
config cifs domain-controller
   Description: Define known domain controller servers.
   edit <server-name>
      set domain-name {string}
      set username {string}
      set password {password}
      set port {integer}
      set ip {ipv4-address-any}
      set ip6 {ipv6-address}
   next
end
```

config cifs domain-controller

Parameter	Description	Type	Size
domain-name	Fully qualified domain name (FQDN). E.g. 'EXAMPLE.COM'.	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
port	Port number of service. Port number 0 indicates automatic discovery.	integer	Minimum value: 0 Maximum value: 65535
ip	IPv4 server address.	ipv4-address-any	Not Specified
ip6	IPv6 server address.	ipv6-address	Not Specified

config cifs profile

Configure CIFS profile.

```
config cifs profile
   Description: Configure CIFS profile.
   edit <name>
      config file-filter
         Description: File filter.
         set status [enable|disable]
         set log [enable|disable]
         config entries
            Description: File filter entries.
            edit <filter>
               set comment {var-string}
               set action [log|block]
               set direction [incoming|outgoing|...]
               set file-type <name1>, <name2>, ...
            next
         end
      end
      set domain-controller {string}
      set server-credential-type [none|credential-replication|...]
      config server-keytab
         Description: Server keytab.
         edit <principal>
            set keytab {string}
         next
      end
   next
end
```

config cifs profile

Parameter	Description	Type	Size
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 255
server-credential-type	CIFS server credential type.	option	-

Option	Description
none	Credential derivation not set.
credential-replication	Credential derived using Replication account on Domain Controller.
credential-keytab	Credential derived using server keytab.

config file-filter

Parameter	Description	Type	Size
status	Enable/disable file filter.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable file filter. *disable* Disable file filter.		
log	Enable/disable file filter logging.	option	-
	Option **Description** *enable* Enable file filter logging. *disable* Disable file filter logging.		

config entries

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
action	Action taken for matched file.	option	-
	Option **Description** *log* Allow the content and write a log message. *block* Block the content and write a log message.		
direction	Match files transmitted in the session's originating or reply direction.	option	-
	Option **Description** *incoming* Match files transmitted in the session's originating direction. *outgoing* Match files transmitted in the session's reply direction. *any* Match files transmitted in the session's originating and reply direction.		
file-type <name>	Select file type. File type name.	string	Maximum length: 39

config server-keytab

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

dlp

This section includes syntax for the following commands:

- config dlp sensor on page 86
- config dlp filepattern on page 83
- config dlp sensitivity on page 86

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
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
filter-type	Filter by file name pattern or by file type.	option	-

Option	Description
pattern	Filter by file name pattern.
type	Filter by file type.

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

Option	Description
7z	Match 7-zip files.
arj	Match arj compressed files.
cab	Match Windows cab files.
lzh	Match lzh compressed files.
rar	Match rar archives.
tar	Match tar files.
zip	Match zip files.
bzip	Match bzip files.
gzip	Match gzip files.
bzip2	Match bzip2 files.
xz	Match xz files.
bat	Match Windows batch files.
msc	Match msc files.
uue	Match uue files.
mime	Match mime files.
base64	Match base64 files.
binhex	Match binhex files.
elf	Match elf files.
exe	Match Windows executable files.
hta	Match hta files.
html	Match html files.
jad	Match jad files.
class	Match class files.
cod	Match cod files.
javascript	Match javascript files.
msoffice	Match MS-Office files. For example, doc, xls, ppt, and so on.
msofficex	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.
fsg	Match fsg files.

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

Option	Description
crx	Match Chrome extension files.
flac	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 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 options {option}
      set full-archive-proto {option1}, {option2}, ...
      set summary-proto {option1}, {option2}, ...
   next
end
```

config dlp sensor

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
replacemsg-group	Replacement message group used by this DLP sensor.	string	Maximum length: 35
dlp-log	Enable/disable DLP logging.	option	-

Option	Description
enable	Enable DLP logging.
disable	Disable DLP logging.

Parameter	Description	Type	Size
extended-log	Enable/disable extended logging for data leak prevention.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
nac-quar-log	Enable/disable NAC quarantine logging.	option	-

Option	Description
enable	Enable NAC quarantine logging.
disable	Disable NAC quarantine logging.

Parameter	Description	Type	Size
options	Configure DLP options.	option	-
full-archive-proto	Protocols to always content archive.	option	-

Option	Description
smtp	SMTP.
pop3	POP3.
imap	IMAP.
http-get	HTTP GET.
http-post	HTTP POST.
ftp	FTP.
nntp	NNTP.

Parameter	Description	Type	Size
	Option **Description** *mapi* MAPI. *ssh* SFTP and SCP.		
summary-proto	Protocols to always log summary.	option	-
	Option **Description** *smtp* SMTP. *pop3* POP3. *imap* IMAP. *http-get* HTTP GET. *http-post* HTTP POST. *ftp* FTP. *nntp* NNTP. *mapi* MAPI. *ssh* SFTP and SCP.		

config filter

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

Parameter	Description	Type	Size
	Option / **Description** *file* — Check the contents of downloaded or attached files. *message* — Check the contents of email messages, web pages, etc.		
proto	Check messages or files over one or more of these protocols.	option	-
	Option / **Description** *smtp* — SMTP. *pop3* — POP3. *imap* — IMAP. *http-get* — HTTP GET. *http-post* — HTTP POST. *ftp* — FTP. *nntp* — NNTP. *mapi* — MAPI. *ssh* — SFTP and SCP.		
filter-by	Select the type of content to match.	option	-
	Option / **Description** *credit-card* — Match credit cards. *ssn* — Match social security numbers. *regexp* — Use a regular expression to match content. *file-type* — Match a DLP file pattern list. *file-size* — Match any file over with a size over the threshold. *watermark* — Look for defined file watermarks. *encrypted* — Look for encrypted files.		
file-size	Match files this size or larger .	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
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
regexp	Enter a regular expression to match (max. 255 characters).	string	Maximum length: 255
archive	Enable/disable DLP archiving.	option	-

Option	Description
disable	No DLP archiving.
enable	Enable full DLP archiving.

action	Action to take with content that this DLP sensor matches.	option	-

Option	Description
allow	Allow the content to pass through the FortiGate and do not create a log message.
log-only	Allow the content to pass through the FortiGate, but write a log message.
block	Block the content and write a log message.
quarantine-ip	Quarantine all traffic from the IP address and write a log message.

expiry	Quarantine duration in days, hours, minutes format (dddhhmm).	user	Not Specified

dnsfilter

This section includes syntax for the following commands:

- config dnsfilter profile on page 92
- config dnsfilter domain-filter on page 91

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

config entries

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

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

config dnsfilter profile

Configure DNS domain filter profiles.

```
config dnsfilter profile
   Description: Configure DNS domain filter profiles.
   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
comment	Comment.	var-string	Maximum length: 255
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-

Option	Description
enable	Enable logging of all domains visited.
disable	Disable logging of all domains visited.

Parameter	Description	Type	Size
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-

Option	Description
enable	Enable FortiGuard SDNS rating error logging.
disable	Disable FortiGuard SDNS rating error logging.

Parameter	Description	Type	Size
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-

Option	Description
enable	Enable domain filtering and botnet domain logging.
disable	Disable domain filtering and botnet domain logging.

Parameter	Description	Type	Size
block-action	Action to take for blocked domains.	option	-
	Option / **Description** *block* — Return NXDOMAIN for blocked domains. *redirect* — Redirect blocked domains to SDNS portal.		
redirect-portal	IPv4 address of the SDNS redirect portal.	ipv4-address	Not Specified
redirect-portal6	IPv6 address of the SDNS redirect portal.	ipv6-address	Not Specified
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-
	Option / **Description** *disable* — Disable blocking botnet C&C DNS lookups. *enable* — Enable blocking botnet C&C DNS lookups.		
safe-search	Enable/disable Google, Bing, and YouTube safe search.	option	-
	Option / **Description** *disable* — Disable Google, Bing, and YouTube safe search. *enable* — Enable Google, Bing, and YouTube safe search.		
youtube-restrict	Set safe search for YouTube restriction level.	option	-
	Option / **Description** *strict* — Enable strict safe seach for YouTube. *moderate* — 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
domain-filter-table	DNS domain filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295

config ftgd-dns

Parameter	Description	Type	Size
options	FortiGuard DNS filter options.	option	-

Option	Description
error-allow	Allow all domains when FortiGuard DNS servers fail.
ftgd-disable	Disable FortiGuard DNS domain rating.

config filters

Parameter	Description	Type	Size
category	Category number.	integer	Minimum value: 0 Maximum value: 255
action	Action to take for DNS requests matching the category.	option	-

Option	Description
block	Block DNS requests matching the category.
monitor	Allow DNS requests matching the category and log the result.

log	Enable/disable DNS filter logging for this DNS profile.	option	-

Option	Description
enable	Enable DNS filter logging.
disable	Disable DNS filter logging.

config dns-translation

Parameter	Description	Type	Size
addr-type	DNS translation type (IPv4 or IPv6).	option	-

Option	Description
ipv4	IPv4 address type.
ipv6	IPv6 address type.

src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified

Parameter	Description	Type	Size
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
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified
status	Enable/disable this DNS translation entry.	option	-

Option	Description
enable	Enable this DNS translation.
disable	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

emailfilter

This section includes syntax for the following commands:

- config emailfilter iptrust on page 103
- config emailfilter profile on page 104
- config emailfilter options on page 113
- config emailfilter bword on page 97
- config emailfilter bwl on page 99
- config emailfilter mheader on page 101
- config emailfilter fortishield on page 112
- config emailfilter dnsbl on page 102

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

config entries

Parameter	Description	Type	Size
status	Enable/disable status.	option	-

Option	Description
enable	Enable status.
disable	Disable status.

Parameter	Description	Type	Size
pattern	Pattern for the banned word.	string	Maximum length: 127
pattern-type	Wildcard pattern or regular expression.	option	-

Option	Description
wildcard	Wildcard pattern.
regexp	Perl regular expression.

Parameter	Description	Type	Size
action	Mark spam or good.	option	-

Option	Description
spam	Mark as spam email.
clear	Mark as good email.

Parameter	Description	Type	Size
where	Component of the email to be scanned.	option	-

Option	Description
subject	Banned word in email subject.
body	Banned word in email body.
all	Banned word in both subject and body.

Parameter	Description	Type	Size
language	Language for the banned word.	option	-

Option	Description
western	Western.
simch	Simplified Chinese.
trach	Traditional Chinese.
japanese	Japanese.
korean	Korean.
french	French.

Parameter	Description	Type	Size
	Option / **Description** *thai* / Thai. *spanish* / Spanish.		
score	Score value.	integer	Minimum value: 1 Maximum value: 99999

config emailfilter bwl

Configure anti-spam black/white list.

```
config emailfilter bwl
   Description: Configure anti-spam black/white list.
   edit <id>
      set name {string}
      set comment {var-string}
      config entries
         Description: Anti-spam black/white list 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 bwl

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

config entries

Parameter	Description	Type	Size
status	Enable/disable status.	option	-

Option	Description
enable	Enable status.
disable	Disable status.

Parameter	Description	Type	Size
type	Entry type.	option	-

Option	Description
ip	By IP address.
email	By email address.

Parameter	Description	Type	Size
action	Reject, mark as spam or good email.	option	-

Option	Description
reject	Reject the connection.
spam	Mark as spam email.
clear	Mark as good email.

Parameter	Description	Type	Size
addr-type	IP address type.	option	-

Option	Description
ipv4	IPv4 Address type.
ipv6	IPv6 Address type.

Parameter	Description	Type	Size
ip4-subnet	IPv4 network address/subnet mask bits.	ipv4-classnet	Not Specified
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified
pattern-type	Wildcard pattern or regular expression.	option	-

Option	Description
wildcard	Wildcard pattern.
regexp	Perl regular expression.

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

config entries

Parameter	Description	Type	Size
status	Enable/disable status.	option	-

Option	Description
enable	Enable status.
disable	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	-

Parameter	Description	Type	Size
	Option / **Description** *wildcard* / Wildcard pattern. *regexp* / Perl regular expression.		
action	Mark spam or good.	option	-
	Option / **Description** *spam* / Mark as spam email. *clear* / 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
name	Name of table.	string	Maximum length: 63
comment	Optional comments.	var-string	Maximum length: 255

config entries

Parameter	Description	Type	Size
status	Enable/disable status.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable status. *disable* / Disable status.		
server	DNSBL or ORBL server name.	string	Maximum length: 127
action	Reject connection or mark as spam email.	option	-
	Option / **Description** *reject* / Reject the connection. *spam* / 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
name	Name of table.	string	Maximum length: 63
comment	Optional comments.	var-string	Maximum length: 255

config entries

Parameter	Description	Type	Size
status	Enable/disable status.	option	-
	Option / **Description** *enable* / Enable status. *disable* / Disable status.		
addr-type	Type of address.	option	-
	Option / **Description** *ipv4* / IPv4 Address type. *ipv6* / IPv6 Address type.		
ip4-subnet	IPv4 network address or network address/subnet mask bits.	ipv4-classnet	Not Specified
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified

config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
   Description: Configure Email Filter profiles.
   edit <name>
      set comment {var-string}
      set replacemsg-group {string}
      set spam-log [disable|enable]
      set spam-log-fortiguard-response [disable|enable]
      config file-filter
         Description: File filter.
         set status [enable|disable]
         set log [enable|disable]
         set scan-archive-contents [enable|disable]
         config entries
            Description: File filter entries.
            edit <filter>
               set comment {var-string}
               set protocol {option1}, {option2}, ...
               set action [log|block]
               set password-protected [yes|any]
               set file-type <name1>, <name2>, ...
            next
         end
      end
      set spam-filtering [enable|disable]
      set external [enable|disable]
      set options {option1}, {option2}, ...
      config imap
```

```
        Description: IMAP.
        set log [enable|disable]
        set action [pass|tag]
        set tag-type {option1}, {option2}, ...
        set tag-msg {string}
    end
    config pop3
        Description: POP3.
        set log [enable|disable]
        set action [pass|tag]
        set tag-type {option1}, {option2}, ...
        set tag-msg {string}
    end
    config smtp
        Description: SMTP.
        set log [enable|disable]
        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 [enable|disable]
        set action [pass|discard]
    end
    config msn-hotmail
        Description: MSN Hotmail.
        set log [enable|disable]
    end
    config yahoo-mail
        Description: Yahoo! Mail.
        set log [enable|disable]
    end
    config gmail
        Description: Gmail.
        set log [enable|disable]
    end
    set spam-bword-threshold {integer}
    set spam-bword-table {integer}
    set spam-bwl-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
comment	Comment.	var-string	Maximum length: 255

Parameter	Description	Type	Size
replacemsg-group	Replacement message group.	string	Maximum length: 35
spam-log	Enable/disable spam logging for email filtering.	option	-

Option	Description
disable	Disable spam logging for email filtering.
enable	Enable spam logging for email filtering.

Parameter	Description	Type	Size
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-

Option	Description
disable	Disable logging FortiGuard spam response.
enable	Enable logging FortiGuard spam response.

Parameter	Description	Type	Size
spam-filtering	Enable/disable spam filtering.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
external	Enable/disable external Email inspection.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
options	Options.	option	-

Option	Description
bannedword	Content block.
spambwl	Black/white list.
spamfsip	Email IP address FortiGuard AntiSpam black list check.
spamfssubmit	Add FortiGuard AntiSpam spam submission text.
spamfschksum	Email checksum FortiGuard AntiSpam check.
spamfsurl	Email content URL FortiGuard AntiSpam check.
spamhelodns	Email helo/ehlo domain DNS check.

Parameter	Description	Type	Size
	Option / **Description** *spamraddrdns* / Email return address DNS check. *spamrbl* / Email DNSBL & ORBL check. *spamhdrcheck* / Email mime header check. *spamfsphish* / Email content phishing URL FortiGuard AntiSpam check.		
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-bwl-table	Anti-spam black/white list table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-mheader-table	Anti-spam MIME header table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-rbl-table	Anti-spam DNSBL table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 Maximum value: 4294967295

config file-filter

Parameter	Description	Type	Size
status	Enable/disable file filter.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable file filter. *disable* Disable file filter.		
log	Enable/disable file filter logging.	option	-
	Option **Description** *enable* Enable file filter logging. *disable* Disable file filter logging.		
scan-archive-contents	Enable/disable file filter archive contents scan.	option	-
	Option **Description** *enable* Enable file filter archive contents scan. *disable* Disable file filter archive contents scan.		

config entries

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
protocol	Protocols to apply with.	option	-
	Option **Description** *smtp* Enable/disable SMTP. *imap* Enable/disable IMAP. *pop3* Enable/disable POP3.		
action	Action taken for matched file.	option	-
	Option **Description** *log* Allow the content and write a log message. *block* Block the content and write a log message.		
password-protected	Match password-protected files.	option	-

Parameter	Description	Type	Size
	Option **Description** *yes* Match only password-protected files. *any* Match any file.		
file-type <name>	Select file type. File type name.	string	Maximum length: 39

config imap

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

config pop3

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting.		

Parameter	Description	Type	Size
	Option **Description** *disable* Disable setting.		
action	Action for spam email.	option	-
	Option **Description** *pass* Allow spam email to pass through. *tag* Tag spam email with configured text in subject or header.		
tag-type	Tag subject or header for spam email.	option	-
	Option **Description** *subject* Prepend text to spam email subject. *header* Append a user defined mime header to spam email. *spaminfo* Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63

config smtp

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action for spam email.	option	-
	Option **Description** *pass* Allow spam email to pass through. *tag* Tag spam email with configured text in subject or header. *discard* Discard (block) spam email.		
tag-type	Tag subject or header for spam email.	option	-
	Option **Description** *subject* Prepend text to spam email subject.		

Parameter	Description	Type	Size
	Option **Description** *header* Append a user defined mime header to spam email. *spaminfo* Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63
hdrip	Enable/disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.	option	-
	Option **Description** *disable* Disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters. *enable* Enable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.		
local-override	Enable/disable local filter to override SMTP remote check result.	option	-
	Option **Description** *disable* Disable local filter to override SMTP remote check result. *enable* Enable local filter to override SMTP remote check result.		

config mapi

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action for spam email.	option	-
	Option **Description** *pass* Allow spam email to pass through. *discard* Discard (block) spam email.		

config msn-hotmail

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

config yahoo-mail

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

config gmail

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

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
spam-submit-srv	Hostname of the spam submission server.	string	Maximum length: 63
spam-submit-force	Enable/disable force insertion of a new mime entity for the submission text.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
spam-submit-txt2htm	Enable/disable conversion of text email to HTML email.	option	-

Option	Description
enable	Enable setting.
disable	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
dns-timeout	DNS query time out .	integer	Minimum value: 1 Maximum value: 30

endpoint-control

This section includes syntax for the following commands:

- config endpoint-control settings on page 114
- config endpoint-control fctems on page 115

config endpoint-control settings

Configure endpoint control settings.

```
config endpoint-control settings
   Description: Configure endpoint control settings.
   set forticlient-keepalive-interval {integer}
   set forticlient-sys-update-interval {integer}
   set forticlient-user-avatar [enable|disable]
   set forticlient-disconnect-unsupported-client [enable|disable]
end
```

config endpoint-control settings

Parameter	Description	Type	Size
forticlient-keepalive-interval	Interval between two KeepAlive messages from FortiClient .	integer	Minimum value: 20 Maximum value: 300
forticlient-sys-update-interval	Interval between two system update messages from FortiClient .	integer	Minimum value: 30 Maximum value: 1440
forticlient-user-avatar	Enable/disable uploading FortiClient user avatars.	option	-

Option	Description
enable	Allow uploading FortiClient user avatars.
disable	Disable uploading FortiClient user avatars.

forticlient-disconnect-unsupported-client	Enable/disable disconnecting of unsupported FortiClient endpoints.	option	-

Parameter	Description	Type	Size

Option	Description
enable	Enable disconnection of clients on unsupported routes.
disable	Disable disconnection of clients on unsupported routes.

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 server {string}
      set serial-number {string}
      set fortinetone-cloud-authentication [enable|disable]
      set https-port {integer}
      set admin-username {string}
      set admin-password {password}
      set source-ip {ipv4-address-any}
      set call-timeout {integer}
   next
end
```

config endpoint-control fctems

Parameter	Description	Type	Size
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255
serial-number	FortiClient EMS Serial Number.	string	Maximum length: 16
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-

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.

Parameter	Description	Type	Size
https-port	FortiClient EMS HTTPS access port number. .	integer	Minimum value: 1 Maximum value: 65535
admin-username	FortiClient EMS admin username.	string	Maximum length: 128
admin-password	FortiClient EMS admin password.	password	Not Specified
source-ip	REST API call source IP.	ipv4-address-any	Not Specified
call-timeout	FortiClient EMS call timeout in milliseconds .	integer	Minimum value: 500 Maximum value: 30000

extender

This section includes syntax for the following commands:

- config extender sys-info on page 117
- config extender modem-status on page 117

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
<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
<sn>	extender serial number.	string	Maximum length: -1

extender-controller

This section includes syntax for the following commands:

- config extender-controller extender on page 118

config extender-controller extender

Extender controller configuration.

```
config extender-controller extender
   Description: Extender controller configuration.
   edit <id>
      set admin [disable|discovered|...]
      set ifname {string}
      set vdom {integer}
      set role [none|primary|...]
      set mode [standalone|redundant]
      set dial-mode [dial-on-demand|always-connect]
      set redial [none|1|...]
      set redundant-intf {string}
      set dial-status {integer}
      set conn-status {integer}
      set ext-name {string}
      set description {string}
      set quota-limit-mb {integer}
      set billing-start-day {integer}
      set at-dial-script {string}
      set modem-passwd {password}
      set initiated-update [enable|disable]
      set modem-type [cdma|gsm/lte|...]
      set ppp-username {string}
      set ppp-password {password}
      set ppp-auth-protocol [auto|pap|...]
      set ppp-echo-request [enable|disable]
      set wimax-carrier {string}
      set wimax-realm {string}
      set wimax-auth-protocol [tls|ttls]
      set sim-pin {password}
      set access-point-name {string}
      set multi-mode [auto|auto-3g|...]
      set roaming [enable|disable]
      set cdma-nai {string}
      set aaa-shared-secret {password}
      set ha-shared-secret {password}
      set primary-ha {string}
      set secondary-ha {string}
      set cdma-aaa-spi {string}
      set cdma-ha-spi {string}
   next
end
```

config extender-controller extender

Parameter	Description	Type	Size
admin	FortiExtender Administration (enable or disable).	option	-

Option	Description
disable	AC is configured to not provide service to this FortiExtender.
discovered	FortiExtender discovered through discovery or join request message.
enable	AC is configured to provide service to this FortiExtender.

ifname	FortiExtender interface name.	string	Maximum length: 15
vdom	VDOM	integer	Minimum value: 0 Maximum value: 4294967295
role	FortiExtender work role(Primary, Secondary, None).	option	-

Option	Description
none	FortiExtender is not supplying any service.
primary	FortiExtender is supplying primary service.
secondary	FortiExtender is standby for primary FortiExtender.

mode	FortiExtender mode.	option	-

Option	Description
standalone	Standalone.
redundant	Redundant for an interface.

dial-mode	Dial mode (dial-on-demand or always-connect).	option	-

Option	Description
dial-on-demand	The dial action is controlled by user.
always-connect	auto dial.

redial	Number of redials allowed based on failed attempts.	option	-

Option	Description
none	Forever.

Parameter	Description	Type	Size
	Option / **Description** *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.		
redundant-intf	Redundant interface.	string	Maximum length: 15
dial-status	Dial status.	integer	Minimum value: 0 Maximum value: 4294967295
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295
ext-name	FortiExtender name.	string	Maximum length: 31
description	Description.	string	Maximum length: 31
quota-limit-mb	Monthly quota limit (MB).	integer	Minimum value: 0 Maximum value: 10485760
billing-start-day	Billing start day.	integer	Minimum value: 1 Maximum value: 28

Parameter	Description	Type	Size
at-dial-script	Initialization AT commands specific to the MODEM.	string	Maximum length: 127
modem-passwd	MODEM password.	password	Not Specified
initiated-update	Allow/disallow network initiated updates to the MODEM.	option	-

Option	Description
enable	Enable network_initiated_update option.
disable	Disable network_initiated_update option.

modem-type	MODEM type (CDMA, GSM/LTE or WIMAX).	option	-

Option	Description
cdma	CDMA
gsm/lte	GSM/LTE
wimax	WIMAX

ppp-username	PPP username.	string	Maximum length: 31
ppp-password	PPP password.	password	Not Specified
ppp-auth-protocol	PPP authentication protocol (PAP,CHAP or auto).	option	-

Option	Description
auto	AUTO
pap	PAP
chap	CHAP

ppp-echo-request	Enable/disable PPP echo request.	option	-

Option	Description
enable	Enable PPP echo request option.
disable	Disable PPP echo request option.

wimax-carrier	WiMax carrier.	string	Maximum length: 31

Parameter	Description	Type	Size
wimax-realm	WiMax realm.	string	Maximum length: 31
wimax-auth-protocol	WiMax authentication protocol(TLS or TTLS).	option	-

Option	Description
tls	TLS
ttls	TTLS

sim-pin	SIM PIN.	password	Not Specified
access-point-name	Access point name(APN).	string	Maximum length: 63
multi-mode	MODEM mode of operation(3G,LTE,etc).	option	-

Option	Description
auto	AUTO
auto-3g	Auto 3G(3G or less)
force-lte	Force LTE
force-3g	Force 3G
force-2g	Force 2G

roaming	Enable/disable MODEM roaming.	option	-

Option	Description
enable	Enable GSM/LTE roaming option.
disable	Disable GSM/LTE roaming option.

cdma-nai	NAI for CDMA MODEMS.	string	Maximum length: 31
aaa-shared-secret	AAA shared secret.	password	Not Specified
ha-shared-secret	HA shared secret.	password	Not Specified
primary-ha	Primary HA.	string	Maximum length: 31
secondary-ha	Secondary HA.	string	Maximum length: 31

Parameter	Description	Type	Size
cdma-aaa-spi	CDMA AAA SPI.	string	Maximum length: 31
cdma-ha-spi	CDMA HA SPI.	string	Maximum length: 31

firewall

This section includes syntax for the following commands:

- config firewall consolidated policy on page 274
- config firewall interface-policy6 on page 346
- config firewall ipmacbinding table on page 234
- config firewall internet-service-ipbl-vendor on page 155
- config firewall internet-service-sld on page 154
- config firewall local-in-policy on page 313
- config firewall vipgrp on page 230
- config firewall ip-translation on page 365
- config firewall address6 on page 132
- config firewall internet-service-ipbl-reason on page 155
- config firewall shaping-profile on page 311
- config firewall ssh host-key on page 364
- config firewall sniffer on page 353
- config firewall ippool6 on page 170
- config firewall central-snat-map on page 358
- config firewall policy on page 289
- config firewall multicast-policy on page 339
- config firewall shaper per-ip-shaper on page 159
- config firewall multicast-address on page 130
- config firewall wildcard-fqdn custom on page 139
- config firewall local-in-policy6 on page 325
- config firewall vipgrp46 on page 231
- config firewall multicast-policy6 on page 341
- config firewall ldb-monitor on page 170
- config firewall proute6 on page 369
- config firewall DoS-policy6 on page 351
- config firewall ssh setting on page 363
- config firewall iprope appctrl list on page 368
- config firewall shaper per-ip on page 161
- config firewall policy6 on page 315
- config firewall security-policy on page 283
- config firewall ippool on page 168
- config firewall internet-service-custom on page 151
- config firewall internet-service-owner on page 155
- config firewall address on page 126
- config firewall shaping-policy on page 307
- config firewall addrgrp on page 136
- config firewall internet-service-custom-group on page 154
- config firewall vipgrp6 on page 232

- config firewall shaper traffic on page 161
- config firewall ipmacbinding setting on page 233
- config firewall profile-protocol-options on page 235
- config firewall iprope appctrl status on page 368
- config firewall ssl-server on page 270
- config firewall vipgrp64 on page 232
- config firewall service custom on page 141
- config firewall schedule group on page 167
- config firewall internet-service-extension on page 148
- config firewall wildcard-fqdn group on page 140
- config firewall addrgrp6 on page 138
- config firewall service category on page 141
- config firewall policy46 on page 330
- config firewall proute on page 368
- config firewall iprope list on page 368
- config firewall policy64 on page 327
- config firewall multicast-address6 on page 135
- config firewall internet-service-group on page 148
- config firewall vip6 on page 202
- config firewall service group on page 145
- config firewall schedule onetime on page 166
- config firewall internet-service-append on page 153
- config firewall internet-service-definition on page 156
- config firewall vip46 on page 198
- config firewall dnstranslation on page 339
- config firewall identity-based-route on page 272
- config firewall DoS-policy on page 349
- config firewall ssh local-key on page 361
- config firewall vip on page 171
- config firewall vip64 on page 227
- config firewall interface-policy on page 343
- config firewall ssl setting on page 360
- config firewall internet-service-reputation on page 150
- config firewall ttl-policy on page 326
- config firewall proxy-policy on page 333
- config firewall proxy-addrgrp on page 164
- config firewall internet-service-list on page 156
- config firewall profile-group on page 269
- config firewall proxy-address on page 161
- config firewall address6-template on page 131
- config firewall ssh local-ca on page 362
- config firewall ssl-ssh-profile on page 253
- config firewall traffic-class on page 306
- config firewall shaper traffic-shaper on page 157
- config firewall schedule recurring on page 166

- config firewall ipv6-eh-filter on page 366
- config firewall internet-service on page 146
- config firewall internet-service-addition on page 152
- config firewall auth-portal on page 273

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 start-mac {mac-address}
      set end-mac {mac-address}
      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 fsso-group <name1>, <name2>, ...
      set interface {string}
      set tenant {string}
      set organization {string}
      set epg-name {string}
      set subnet-name {string}
      set sdn-tag {string}
      set policy-group {string}
      set comment {var-string}
      set visibility [enable|disable]
      set associated-interface {string}
      set color {integer}
      set filter {var-string}
      set sdn-addr-type [private|public|...]
      set obj-id {var-string}
      config list
         Description: IP address list.
         edit <ip>
         next
      end
      config tagging
         Description: Config object tagging.
         edit <name>
            set category {string}
            set tags <name1>, <name2>, ...
         next
      end
      set allow-routing [enable|disable]
```

```
    next
end
```

config firewall address

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified
type	Type of address.	option	-

Option	Description
ipmask	Standard IPv4 address with subnet mask.
iprange	Range of IPv4 addresses between two specified addresses (inclusive).
fqdn	Fully Qualified Domain Name address.
geography	IP addresses from a specified country.
wildcard	Standard IPv4 using a wildcard subnet mask.
dynamic	Dynamic address object.
interface-subnet	IP and subnet of interface.
mac	Range of MAC addresses.

sub-type	Sub-type of address.	option	-

Option	Description
sdn	SDN address.
clearpass-spt	ClearPass SPT (System Posture Token) address.
fsso	FSSO address.

clearpass-spt	SPT (System Posture Token) value.	option	-

Option	Description
unknown	UNKNOWN.
healthy	HEALTHY.
quarantine	QUARANTINE.
checkup	CHECKUP.
transient	TRANSIENT.
infected	INFECTED.

Parameter	Description	Type	Size
start-mac	First MAC address in the range.	mac-address	Not Specified
end-mac	Last MAC address in the range.	mac-address	Not Specified
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified
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
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified
sdn	SDN.	string	Maximum length: 35
fsso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35
tenant	Tenant.	string	Maximum length: 35
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35
epg-name	Endpoint group name.	string	Maximum length: 255
subnet-name	Subnet name.	string	Maximum length: 255
sdn-tag	SDN Tag.	string	Maximum length: 15
policy-group	Policy group name.	string	Maximum length: 15

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
visibility	Enable/disable address visibility in the GUI.	option	-

Option	Description
enable	Show in address4 selection.
disable	Hide from address4 selection.

Parameter	Description	Type	Size
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
filter	Match criteria filter.	var-string	Maximum length: 2047
sdn-addr-type	Type of addresses to collect.	option	-

Option	Description
private	Collect private addresses only.
public	Collect public addresses only.
all	Collect both public and private addresses.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable use of this address in the static route configuration.
disable	Disable use of this address in the static route configuration.

config tagging

Parameter	Description	Type	Size
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 visibility [enable|disable]
      set associated-interface {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-address

Parameter	Description	Type	Size
type	Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.	option	-

Option	Description
multicastrange	Multicast range.
broadcastmask	Broadcast IP/mask.

subnet	Broadcast address and subnet.	ipv4-classnet-any	Not Specified
start-ip	First IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified
end-ip	Final IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified
comment	Comment.	var-string	Maximum length: 255
visibility	Enable/disable visibility of the multicast address on the GUI.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Show the multicast address on the GUI. *disable* — Hide the multicast address from the GUI.		
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

config tagging

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

config firewall address6-template

Configure IPv6 address templates.

```
config firewall address6-template
   Description: Configure IPv6 address templates.
   edit <name>
      set 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
   next
end
```

config firewall address6-template

Parameter	Description	Type	Size
ip6	IPv6 address prefix.	ipv6-network	Not Specified
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6

config subnet-segment

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

Option	Description
enable	Enable exclusive value.
disable	Disable exclusive value.

config values

Parameter	Description	Type	Size
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 start-mac {mac-address}
      set end-mac {mac-address}
      set sdn {string}
      set ip6 {ipv6-network}
      set start-ip {ipv6-address}
```

```
      set end-ip {ipv6-address}
      set fqdn {string}
      set cache-ttl {integer}
      set visibility [enable|disable]
      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}
   next
end
```

config firewall address6

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
type	Type of IPv6 address object .	option	-

Option	Description
ipprefix	Uses the IP prefix to define a range of IPv6 addresses.
iprange	Range of IPv6 addresses between two specified addresses (inclusive).
fqdn	Fully qualified domain name.
dynamic	Dynamic address object for SDN.
template	Template.
mac	Range of MAC addresses.

Parameter	Description	Type	Size
start-mac	First MAC address in the range.	mac-address	Not Specified
end-mac	Last MAC address in the range.	mac-address	Not Specified
sdn	SDN.	string	Maximum length: 35
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified
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
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400
visibility	Enable/disable the visibility of the object in the GUI.	option	-

Option	Description
enable	Show in address6 selection.
disable	Hide from address6 selection.

color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32
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	-

Option	Description
any	Wildcard.

Parameter	Description	Type	Size
	Option / **Description** *specific* / Specific host address.		
host	Host Address.	ipv6-address	Not Specified

config tagging

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

config subnet-segment

Parameter	Description	Type	Size
type	Subnet segment type.	option	-
	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 visibility [enable|disable]
      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
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified
comment	Comment.	var-string	Maximum length: 255
visibility	Enable/disable visibility of the IPv6 multicast address on the GUI.	option	-

Option	Description
enable	Show the IPv6 multicast address on the GUI.
disable	Hide the IPv6 multicast address from the GUI.

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

config tagging

Parameter	Description	Type	Size
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 uuid {uuid}
      set member <name1>, <name2>, ...
      set comment {var-string}
      set exclude [enable|disable]
      set exclude-member <name1>, <name2>, ...
      set visibility [enable|disable]
      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]
  next
end
```

config firewall addrgrp

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
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	-
	Option / **Description** *enable* — Enable address exclusion. *disable* — Disable address exclusion.		
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79
visibility	Enable/disable address visibility in the GUI.	option	-
	Option / **Description** *enable* — Show in address group selection. *disable* — Hide from address group selection.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
allow-routing	Enable/disable use of this group in the static route configuration.	option	-
	Option / **Description** *enable* — Enable use of this group in the static route configuration. *disable* — Disable use of this group in the static route configuration.		

config tagging

Parameter	Description	Type	Size
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 visibility [enable|disable]
      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
   next
end
```

config firewall addrgrp6

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable address group6 visibility in the GUI.	option	-

Option	Description
enable	Show in address group selection.
disable	Hide from address group selection.

color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79

config tagging

Parameter	Description	Type	Size
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}
      set visibility [enable|disable]
   next
end
```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255

Parameter	Description	Type	Size
visibility	Enable/disable address visibility.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

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}
      set visibility [enable|disable]
   next
end
```

config firewall wildcard-fqdn group

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
member <name>	Address group members. Address name.	string	Maximum length: 79
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
visibility	Enable/disable address visibility.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

config firewall service category

Configure service categories.

```
config firewall service category
   Description: Configure service categories.
   edit <name>
      set comment {var-string}
   next
end
```

config firewall service category

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

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 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>, ...
   next
end
```

config firewall service custom

Parameter	Description	Type	Size
proxy	Enable/disable web proxy service.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
category	Service category.	string	Maximum length: 63
protocol	Protocol type based on IANA numbers.	option	-

Option	Description
TCP/UDP/SCTP	TCP, UDP and SCTP.
ICMP	ICMP.
ICMP6	ICMP6.
IP	IP.
HTTP	HTTP - for web proxy.
FTP	FTP - for web proxy.
CONNECT	Connect - for web proxy.
SOCKS-TCP	Socks TCP - for web proxy.
SOCKS-UDP	Socks UDP - for web proxy.
ALL	All - for web proxy.

Parameter	Description	Type	Size
helper	Helper name.	option	-

Option	Description
auto	Automatically select helper based on protocol and port.
disable	Disable helper.
ftp	FTP.
tftp	TFTP.
ras	RAS.
h323	H323.
tns	TNS.
mms	MMS.

Parameter	Description	Type	Size
	Option **Description** *sip* SIP. *pptp* PPTP. *rtsp* RTSP. *dns-udp* DNS UDP. *dns-tcp* DNS TCP. *pmap* PMAP. *rsh* RSH. *dcerpc* DCERPC. *mgcp* 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
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255
tcp-portrange	Multiple TCP port ranges.	user	Not Specified
udp-portrange	Multiple UDP port ranges.	user	Not Specified
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet .	integer	Minimum value: 0 Maximum value: 86400

Parameter	Description	Type	Size
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet .	integer	Minimum value: 0 Maximum value: 86400
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds .	integer	Minimum value: 0 Maximum value: 300
udp-idle-timer	UDP half close timeout .	integer	Minimum value: 0 Maximum value: 86400
session-ttl	Session TTL .	user	Not Specified
check-reset-range	Configure the type of ICMP error message verification.	option	-

Option	Description
disable	Disable RST range check.
strict	Check RST range strictly.
default	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
visibility	Enable/disable the visibility of the service on the GUI.	option	-

Option	Description
enable	Show in service selection.
disable	Hide from service selection.

app-service-type	Application service type.	option	-

Option	Description
disable	Disable application type.

Parameter	Description	Type	Size
	Option / **Description** *app-id* / Application ID. *app-category* / 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

config firewall service group

Configure service groups.

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

config firewall service group

Parameter	Description	Type	Size
member <name>	Service objects contained within the group. Address name.	string	Maximum length: 79
proxy	Enable/disable web proxy service group.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
comment	Comment.	var-string	Maximum length: 255

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

config firewall internet-service

Show Internet Service application.

```
config firewall internet-service
   Description: Show Internet Service application.
   edit <id>
      set name {string}
      set reputation {integer}
      set icon-id {integer}
      set sld-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
name	Internet Service name.	string	Maximum length: 63
reputation	Reputation level of the Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295
icon-id	Icon ID of Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
sld-id	Second Level Domain.	integer	Minimum value: 0 Maximum value: 4294967295
direction	How this service may be used in a firewall policy (source, destination or both).	option	-

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	-

Option	Description
isdb	Internet Service Database.
irdb	Internet RRR Database.

ip-range-number	Number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295
extra-ip-range-number	Extra number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295
ip-number	Total number of IP addresses.	integer	Minimum value: 0 Maximum value: 4294967295
singularity	Singular level of the Internet Service.	integer	Minimum value: 0 Maximum value: 65535
obsolete	Indicates whether the Internet Service can be used.	integer	Minimum value: 0 Maximum value: 255

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 <id1>, <id2>, ...
   next
end
```

config firewall internet-service-group

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

Option	Description
source	As source when applied.
destination	As destination when applied.
both	Both directions when applied.

member <id>	Internet Service group member. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295

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
      next
   end
next
end
```

config firewall internet-service-extension

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

config entry

Parameter	Description	Type	Size
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255
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
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535

config disable-entry

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

config port-range

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

config ip-range

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

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
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
reputation	Reputation level of the custom Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295
comment	Comment.	var-string	Maximum length: 255

config entry

Parameter	Description	Type	Size
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255
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
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535

config firewall internet-service-addition

Configure Internet Services Addition.

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

config firewall internet-service-addition

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

config entry

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

config port-range

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

Parameter	Description	Type	Size
append-port	Appending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535

config firewall internet-service-custom-group

Configure custom Internet Service group.

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

config firewall internet-service-custom-group

Parameter	Description	Type	Size
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
name	Second Level Domain name.	string	Maximum length: 63

config firewall internet-service-ipbl-vendor

IP blacklist vendor.

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

config firewall internet-service-ipbl-vendor

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

config firewall internet-service-ipbl-reason

IP blacklist reason.

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

config firewall internet-service-ipbl-reason

Parameter	Description	Type	Size
name	IP blacklist 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
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
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
category-id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Internet Service name.	string	Maximum length: 63
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255

config port-range

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

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
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper . Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000
maximum-bandwidth	Upper bandwidth limit enforced by this shaper . 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-

Option	Description
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.

Parameter	Description	Type	Size
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-

Option	Description
low	Low priority.
medium	Medium priority.
high	High priority.

Parameter	Description	Type	Size
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	-

Option	Description
disable	All referring policies share one traffic shaper.
enable	Each referring policy has its own traffic shaper.

Parameter	Description	Type	Size
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable setting traffic DiffServ. *disable* — Disable setting traffic DiffServ.		
diffservcode	DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified
dscp-marking-method	Select DSCP marking method.	option	-
	Option / **Description** *multi-stage* — Multistage marking. *static* — 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
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
exceed-class-id	Class ID for traffic in [guaranteed-bandwidth, maximum-bandwidth].	integer	Minimum value: 0 Maximum value: 4294967295

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 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
max-bandwidth	Upper bandwidth limit enforced by this shaper . 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-

Option	Description
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.

max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper . 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.	option	-

Option	Description
enable	Enable setting forward (original) traffic DiffServ.
disable	Disable setting forward (original) traffic DiffServ.

diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-

Option	Description
enable	Enable setting reverse (reply) traffic DiffServ.
disable	Disable setting reverse (reply) traffic DiffServ.

diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified

Parameter	Description	Type	Size
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}
    set visibility [enable|disable]
  next
end
```

config firewall proxy-address

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
type	Proxy address type.	option	-

Option	Description
host-regex	Host regular expression.
url	HTTP URL.
category	FortiGuard URL catgegory.
method	HTTP request method.
ua	HTTP request user agent.
header	HTTP request header.
src-advanced	HTTP advanced source criteria.
dst-advanced	HTTP advanced destination criteria.

Parameter	Description	Type	Size
host	Address object for the host.	string	Maximum length: 79
host-regex	Host name as a regular expression.	string	Maximum length: 255
path	URL path as a regular expression.	string	Maximum length: 255
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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
get	GET method.
post	POST method.
put	PUT method.
head	HEAD method.
connect	CONNECT method.
trace	TRACE method.
options	OPTIONS method.
delete	DELETE method.

ua	Names of browsers to be used as user agent.	option	-

Option	Description
chrome	Google Chrome.
ms	Microsoft Internet Explorer or EDGE.
firefox	Mozilla Firefox.
safari	Apple Safari.
other	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	-

Option	Description
disable	Case insensitive in pattern.
enable	Case sensitive in pattern.

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

Option	Description
enable	Enable setting.
disable	Disable setting.

config header-group

Parameter	Description	Type	Size
header-name	HTTP header.	string	Maximum length: 79
header	HTTP header regular expression.	string	Maximum length: 255
case-sensitivity	Case sensitivity in pattern.	option	-

Option	Description
disable	Case insensitive in pattern.
enable	Case sensitive in pattern.

config tagging

Parameter	Description	Type	Size
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}
      set visibility [enable|disable]
   next
end
```

config firewall proxy-addrgrp

Parameter	Description	Type	Size
type	Source or destination address group type.	option	-
	Option / **Description** *src* — Source group. *dst* — Destination group.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
member <name>	Members of address group. Address name.	string	Maximum length: 79
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32
comment	Optional comments.	var-string	Maximum length: 255
visibility	Enable/disable visibility of the object in the GUI.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		

config tagging

Parameter	Description	Type	Size
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}
   next
end
```

config firewall schedule onetime

Parameter	Description	Type	Size
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
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100

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}
   next
end
```

config firewall schedule recurring

Parameter	Description	Type	Size
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	-

Option	Description
sunday	Sunday.
monday	Monday.
tuesday	Tuesday.
wednesday	Wednesday.
thursday	Thursday.
friday	Friday.
saturday	Saturday.
none	None.

color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32

config firewall schedule group

Schedule group configuration.

```
config firewall schedule group
   Description: Schedule group configuration.
   edit <name>
      set member <name1>, <name2>, ...
      set color {integer}
   next
end
```

config firewall schedule group

Parameter	Description	Type	Size
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

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 source-startip {ipv4-address-any}
      set source-endip {ipv4-address-any}
      set block-size {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}
   next
end
```

config firewall ippool

Parameter	Description	Type	Size
type	IP pool type (overload, one-to-one, fixed port range, or port block allocation).	option	-

Option	Description
overload	IP addresses in the IP pool can be shared by clients.
one-to-one	One to one mapping.
fixed-port-range	Fixed port range.
port-block-allocation	Port block allocation.

Parameter	Description	Type	Size
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
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
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
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
block-size	Number of addresses in a block .	integer	Minimum value: 64 Maximum value: 4096
num-blocks-per-user	Number of addresses blocks that can be used by a user .	integer	Minimum value: 1 Maximum value: 128
pba-timeout	Port block allocation timeout (seconds).	integer	Minimum value: 3 Maximum value: 300
permit-any-host	Enable/disable full cone NAT.	option	-

Option	Description
disable	Disable full cone NAT.
enable	Enable full cone NAT.

arp-reply	Enable/disable replying to ARP requests when an IP Pool is added to a policy .	option	-

Option	Description
disable	Disable ARP reply.
enable	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

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

config firewall ippool6

Configure IPv6 IP pools.

```
config firewall ippool6
   Description: Configure IPv6 IP pools.
   edit <name>
      set startip {ipv6-address}
      set endip {ipv6-address}
      set comments {var-string}
   next
end
```

config firewall ippool6

Parameter	Description	Type	Size
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

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 http-get {string}
      set http-match {string}
      set http-max-redirects {integer}
   next
end
```

config firewall ldb-monitor

Parameter	Description	Type	Size
type	Select the Monitor type used by the health check monitor to check the health of the server (PING | TCP | HTTP | HTTPS).	option	-

Option	Description
ping	PING health monitor.
tcp	TCP-connect health monitor.
http	HTTP-GET health monitor.
https	HTTP-GET health monitor with SSL.

interval	Time between health checks .	integer	Minimum value: 5 Maximum value: 65535
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
retry	Number health check attempts before the server is considered down .	integer	Minimum value: 1 Maximum value: 255
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
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
http-max-redirects	The maximum number of HTTP redirects to be allowed .	integer	Minimum value: 0 Maximum value: 5

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 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 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 ip {ipv4-address-any}
         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 {string}
         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}
   next
end
```

config firewall vip

Parameter	Description	Type	Size
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
comment	Comment.	var-string	Maximum length: 255
type	Configure a static NAT, load balance, server load balance, DNS translation, or FQDN VIP.	option	-

Option	Description
static-nat	Static NAT.
load-balance	Load balance.
server-load-balance	Server load balance.
dns-translation	DNS translation.
fqdn	Fully qualified domain name.

Parameter	Description	Type	Size
dns-mapping-ttl	DNS mapping TTL .	integer	Minimum value: 0 Maximum value: 604800
ldb-method	Method used to distribute sessions to real servers.	option	-

Option	Description
static	Distribute to server based on source IP.
round-robin	Distribute to server based round robin order.
weighted	Distribute to server based on weight.
least-session	Distribute to server with lowest session count.
least-rtt	Distribute to server with lowest Round-Trip-Time.
first-alive	Distribute to the first server that is alive.
http-host	Distribute to server based on host field in HTTP header.

Parameter	Description	Type	Size
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
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	-

Option	Description
disable	Disable ARP reply.
enable	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
http	HTTP
https	HTTPS
imaps	IMAPS
pop3s	POP3S
smtps	SMTPS
ssl	SSL

Parameter	Description	Type	Size
	Option / **Description** *tcp* / TCP *udp* / UDP *ip* / IP		
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-
	Option / **Description** *enable* / Enable redirection of HTTP to HTTPS. *disable* / 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	-
	Option / **Description** *none* / None. *http-cookie* / HTTP cookie. *ssl-session-id* / SSL session ID.		
nat-source-vip	Enable/disable forcing the source NAT mapped IP to the external IP for all traffic.	option	-
	Option / **Description** *disable* / Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP. *enable* / Force the source NAT mapped IP to the external IP for all traffic.		
portforward	Enable/disable port forwarding.	option	-
	Option / **Description** *disable* / Disable port forward. *enable* / Enable port forward.		
protocol	Protocol to use when forwarding packets.	option	-
	Option / **Description** *tcp* / TCP. *udp* / UDP.		

Parameter	Description	Type	Size
	Option / **Description** *sctp* / SCTP. *icmp* / 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
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	-
	Option / **Description** *1-to-1* / One to one. *m-to-n* / Many to many.		
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-
	Option / **Description** *disable* / Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting). *enable* / Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 seconds. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600
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	-

Option	Description
disable	Only allow HTTP cookie to match this virtual server.
same-ip	Allow HTTP cookie to match any virtual server with same IP.

https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-

Option	Description
disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.
enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.

http-multiplex	Enable/disable HTTP multiplexing.	option	-

Option	Description
enable	Enable HTTP session multiplexing.
disable	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	-

Option	Description
enable	Enable adding HTTP header.
disable	Disable adding HTTP header.

http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable Outlook Web Access support. *enable* — Enable Outlook Web Access support.		
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-
	Option / **Description** *disable* — Do not add HTTP header indicating SSL offload for WebLogic server. *enable* — 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	-
	Option / **Description** *disable* — Do not add HTTP header indicating SSL offload for WebSphere server. *enable* — 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	-
	Option / **Description** *half* — Client to FortiGate SSL. *full* — Client to FortiGate and FortiGate to Server SSL.		
ssl-certificate	The name of the SSL certificate to use for SSL acceleration.	string	Maximum length: 35
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-
	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.		

Parameter	Description	Type	Size
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-

Option	Description
high	High encryption. Allow only AES and ChaCha.
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
custom	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.

Parameter	Description	Type	Size
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-

Option	Description
high	High encryption. Allow only AES and ChaCha.
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
custom	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.
client	Use the same encryption algorithms for both client and server sessions.

Parameter	Description	Type	Size
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-

Option	Description
require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.
deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.
allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.

Parameter	Description	Type	Size
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-

Option	Description
ssl-3.0	SSL 3.0.
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.

Parameter	Description	Type	Size
	Option / **Description** *tls-1.2* / TLS 1.2. *tls-1.3* / TLS 1.3.		
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-
	Option / **Description** *ssl-3.0* / SSL 3.0. *tls-1.0* / TLS 1.0. *tls-1.1* / TLS 1.1. *tls-1.2* / TLS 1.2. *tls-1.3* / TLS 1.3.		
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-
	Option / **Description** *ssl-3.0* / SSL 3.0. *tls-1.0* / TLS 1.0. *tls-1.1* / TLS 1.1. *tls-1.2* / TLS 1.2. *tls-1.3* / TLS 1.3. *client* / Use same value as client configuration.		
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-
	Option / **Description** *ssl-3.0* / SSL 3.0. *tls-1.0* / TLS 1.0. *tls-1.1* / TLS 1.1. *tls-1.2* / TLS 1.2. *tls-1.3* / TLS 1.3. *client* / Use same value as client configuration.		

Parameter	Description	Type	Size
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	-

Option	Description
enable	Send empty fragments.
disable	Do not send empty fragments.

Parameter	Description	Type	Size
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-

Option	Description
disable	Disable.
enable	Enable.

Parameter	Description	Type	Size
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-

Option	Description
allow	Allow a SSL client to renegotiate.
deny	Abort any client initiated SSL re-negotiation attempt.
secure	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.

Parameter	Description	Type	Size
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-

Option	Description
disable	Do not keep session states.
time	Expire session states after this many minutes.
count	Expire session states when this maximum is reached.
both	Expire session states based on time or count, whichever occurs first.

Parameter	Description	Type	Size
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400

Parameter	Description	Type	Size
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-

Option	Description
disable	Do not keep session states.
time	Expire session states after this many minutes.
count	Expire session states when this maximum is reached.
both	Expire session states based on time or count, whichever occurs first.

ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-

Option	Description
enable	Enable HTTP location conversion.
disable	Disable HTTP location conversion.

ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-

Option	Description
enable	Match HTTP host in response header.
disable	Do not match HTTP host.

Parameter	Description	Type	Size
ssl-hpkp	Enable/disable including HPKP header in response.	option	-

Option	Description
disable	Do not add a HPKP header to each HTTP response.
enable	Add a HPKP header to each a HTTP response.
report-only	Add a HPKP Report-Only header to each HTTP response.

ssl-hpkp-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
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	-

Option	Description
disable	HPKP header does not apply to subdomains.
enable	HPKP header applies to subdomains.

ssl-hsts	Enable/disable including HSTS header in response.	option	-

Option	Description
disable	Do not add a HSTS header to each a HTTP response.
enable	Add a HSTS header to each HTTP response.

ssl-hsts-age	Number of seconds the client should honour the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — HSTS header does not apply to subdomains. *enable* — 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
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32

config realservers

Parameter	Description	Type	Size
ip	IP address of the real server.	ipv4-address-any	Not Specified
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-
	Option / **Description** *active* — Server status active. *standby* — Server status standby. *disable* — Server status disable.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255

Parameter	Description	Type	Size
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
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-

Option	Description
disable	Disable per server health check.
enable	Enable per server health check.
vip	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
monitor	Name of the health check monitor to use when polling to determine a virtual server's connectivity status.	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
cipher	Cipher suite name.	option	-

Option	Description
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.

Parameter	Description	Type	Size

Option	Description
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

Option	Description
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
TLS-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-RSA-WITH-RC4-128-MD5	Cipher suite TLS-RSA-WITH-RC4-128-MD5.

Parameter	Description	Type	Size
	Option / **Description** *TLS-RSA-WITH-RC4-128-SHA* — Cipher suite TLS-RSA-WITH-RC4-128-SHA. *TLS-DHE-RSA-WITH-DES-CBC-SHA* — Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA. *TLS-DHE-DSS-WITH-DES-CBC-SHA* — Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA. *TLS-RSA-WITH-DES-CBC-SHA* — Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
versions	SSL/TLS versions that the cipher suite can be used with.	option	-
	Option / **Description** *ssl-3.0* — SSL 3.0. *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2. *tls-1.3* — TLS 1.3.		

config ssl-server-cipher-suites

Parameter	Description	Type	Size
cipher	Cipher suite name.	option	-
	Option / **Description** *TLS-AES-128-GCM-SHA256* — Cipher suite TLS-AES-128-GCM-SHA256. *TLS-AES-256-GCM-SHA384* — Cipher suite TLS-AES-256-GCM-SHA384. *TLS-CHACHA20-POLY1305-SHA256* — Cipher suite TLS-CHACHA20-POLY1305-SHA256.		

Parameter	Description	Type	Size

Option	Description
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

Option	Description
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
TLS-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-RSA-WITH-RC4-128-MD5	Cipher suite TLS-RSA-WITH-RC4-128-MD5.

Parameter	Description	Type	Size
	Option / **Description** *TLS-RSA-WITH-RC4-128-SHA* — Cipher suite TLS-RSA-WITH-RC4-128-SHA. *TLS-DHE-RSA-WITH-DES-CBC-SHA* — Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA. *TLS-DHE-DSS-WITH-DES-CBC-SHA* — Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA. *TLS-RSA-WITH-DES-CBC-SHA* — Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
versions	SSL/TLS versions that the cipher suite can be used with.	option	-
	Option / **Description** *ssl-3.0* — SSL 3.0. *tls-1.0* — TLS 1.0. *tls-1.1* — TLS 1.1. *tls-1.2* — TLS 1.2. *tls-1.3* — TLS 1.3.		

config firewall vip46

Configure IPv4 to IPv6 virtual IPs.

```
config firewall vip46
   Description: Configure IPv4 to IPv6 virtual IPs.
   edit <name>
      set id {integer}
      set uuid {uuid}
      set srcintf-filter <interface-name1>, <interface-name2>, ...
      set comment {var-string}
      set type [static-nat|server-load-balance]
      set src-filter <range1>, <range2>, ...
      set extip {user}
      set mappedip {user}
      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|tcp|...]
      config realservers
         Description: Real servers.
         edit <id>
            set ip {ipv6-address}
            set port {integer}
            set status [active|standby|...]
            set weight {integer}
            set holddown-interval {integer}
            set healthcheck [disable|enable|...]
            set max-connections {integer}
            set monitor {string}
            set client-ip {user}
         next
      end
      set monitor <name1>, <name2>, ...
   next
end
```

config firewall vip46

Parameter	Description	Type	Size
id	Custom defined id.	integer	Minimum value: 0 Maximum value: 65535
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
srcintf-filter <interface-name>	Interfaces to which the VIP46 applies. Separate the names with spaces. Interface name.	string	Maximum length: 79
comment	Comment.	var-string	Maximum length: 255
type	VIP type: static NAT or server load balance.	option	-
	Option / **Description** *static-nat* — Static NAT. *server-load-balance* — Server load balance.		
src-filter <range>	Source IP filter (x.x.x.x/x). Src-filter range.	string	Maximum length: 79
extip	Start-external-IP [-end-external-IP].	user	Not Specified

Parameter	Description	Type	Size
mappedip	Start-mapped-IP [-end mapped-IP].	user	Not Specified
arp-reply	Enable ARP reply.	option	-

Option	Description
disable	Disable ARP reply.
enable	Enable ARP reply.

portforward	Enable port forwarding.	option	-

Option	Description
disable	Disable port forwarding.
enable	Enable port forwarding.

protocol	Mapped port protocol.	option	-

Option	Description
tcp	TCP.
udp	UDP.

extport	External service port.	user	Not Specified
mappedport	Mapped service port.	user	Not Specified
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
ldb-method	Load balance method.	option	-

Option	Description
static	Distribute sessions based on source IP.
round-robin	Distribute sessions based round robin order.
weighted	Distribute sessions based on weight.
least-session	Distribute sessions to the server with the lowest session count.
least-rtt	Distribute sessions to the server with the lowest Round-Trip-Time.
first-alive	Distribute sessions to the first server that is alive.

server-type	Server type.	option	-

Parameter	Description	Type	Size
	Option / **Description** *http* / HTTP *tcp* / TCP *udp* / UDP *ip* / IP		
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79

config realservers

Parameter	Description	Type	Size
ip	Mapped server IPv6.	ipv6-address	Not Specified
port	Mapped server port.	integer	Minimum value: 1 Maximum value: 65535
status	Server administrative status.	option	-
	Option / **Description** *active* / Server status active. *standby* / Server status standby. *disable* / Server status disable.		
weight	weight	integer	Minimum value: 1 Maximum value: 255
holddown-interval	Hold down interval.	integer	Minimum value: 30 Maximum value: 65535
healthcheck	Per server health check.	option	-
	Option / **Description** *disable* / Disable per server health check. *enable* / Enable per server health check. *vip* / Use health check defined in VIP.		

Parameter	Description	Type	Size
max-connections	Maximum number of connections allowed to server.	integer	Minimum value: 0 Maximum value: 2147483647
monitor	Health monitors.	string	Maximum length: 79
client-ip	Restrict server to a client IP in this range.	user	Not Specified

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 <range1>, <range2>, ...
      set extip {user}
      set mappedip {user}
      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|...]
      config realservers
         Description: Select the real servers that this server load balancing VIP will
              distribute traffic to.
         edit <id>
            set ip {ipv6-address}
            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 {string}
            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}
  next
end
```

config firewall vip6

Parameter	Description	Type	Size
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
comment	Comment.	var-string	Maximum length: 255
type	Configure a static NAT or server load balance VIP.	option	-

Option	Description
static-nat	Static NAT.
server-load-balance	Server load balance.

src-filter <range>	Source IP6 filter (x:x:x:x:x:x:x:x/x). Separate addresses with spaces. Source-filter range.	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
mappedip	Mapped IP address range in the format startIP-endIP.	user	Not Specified
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-

Option	Description
disable	Disable ARP reply.
enable	Enable ARP reply.

portforward	Enable port forwarding.	option	-

Option	Description
disable	Disable port forward.
enable	Enable/disable port forwarding.

Parameter	Description	Type	Size
protocol	Protocol to use when forwarding packets.	option	-

Option	Description
tcp	TCP.
udp	UDP.
sctp	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
ldb-method	Method used to distribute sessions to real servers.	option	-

Option	Description
static	Distribute sessions based on source IP.
round-robin	Distribute sessions based round robin order.
weighted	Distribute sessions based on weight.
least-session	Sends new sessions to the server with the lowest session count.
least-rtt	Distribute new sessions to the server with lowest Round-Trip-Time.
first-alive	Distribute sessions to the first server that is alive.
http-host	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
http	HTTP
https	HTTPS
imaps	IMAPS
pop3s	POP3S
smtps	SMTPS
ssl	SSL

Parameter	Description	Type	Size
	Option / **Description** *tcp* / TCP *udp* / UDP *ip* / IP		
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-
	Option / **Description** *enable* / Enable redirection of HTTP to HTTPS. *disable* / 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	-
	Option / **Description** *none* / None. *http-cookie* / HTTP cookie. *ssl-session-id* / SSL session ID.		
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-
	Option / **Description** *disable* / Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting). *enable* / Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 seconds. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600
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	-

Option	Description
disable	Only allow HTTP cookie to match this virtual server.
same-ip	Allow HTTP cookie to match any virtual server with same IP.

https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-

Option	Description
disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.
enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.

http-multiplex	Enable/disable HTTP multiplexing.	option	-

Option	Description
enable	Enable HTTP session multiplexing.
disable	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	-

Option	Description
enable	Enable adding HTTP header.
disable	Disable adding HTTP header.

http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable Outlook Web Access support. *enable* — Enable Outlook Web Access support.		
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-
	Option / **Description** *disable* — Do not add HTTP header indicating SSL offload for WebLogic server. *enable* — 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	-
	Option / **Description** *disable* — Do not add HTTP header indicating SSL offload for WebSphere server. *enable* — 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	-
	Option / **Description** *half* — Client to FortiGate SSL. *full* — Client to FortiGate and FortiGate to Server SSL.		
ssl-certificate	The name of the SSL certificate to use for SSL acceleration.	string	Maximum length: 35
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-
	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.		

Parameter	Description	Type	Size
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-

Option	Description
high	Use AES or 3DES.
medium	Use AES, 3DES, or RC4.
low	Use AES, 3DES, RC4, or DES.
custom	Use config ssl-cipher-suites to select the cipher suites that are allowed.

Parameter	Description	Type	Size
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-

Option	Description
high	Use AES or 3DES.
medium	Use AES, 3DES, or RC4.
low	Use AES, 3DES, RC4, or DES.
custom	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.
client	Use the same encryption algorithms for client and server sessions.

Parameter	Description	Type	Size
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-

Option	Description
require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.
deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.
allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.

Parameter	Description	Type	Size
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-

Option	Description
ssl-3.0	SSL 3.0.
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.
tls-1.2	TLS 1.2.

Parameter	Description	Type	Size
	Option **Description** *tls-1.3* TLS 1.3.		
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-
	Option **Description** *ssl-3.0* SSL 3.0. *tls-1.0* TLS 1.0. *tls-1.1* TLS 1.1. *tls-1.2* TLS 1.2. *tls-1.3* TLS 1.3.		
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-
	Option **Description** *ssl-3.0* SSL 3.0. *tls-1.0* TLS 1.0. *tls-1.1* TLS 1.1. *tls-1.2* TLS 1.2. *tls-1.3* TLS 1.3. *client* Use same value as client configuration.		
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-
	Option **Description** *ssl-3.0* SSL 3.0. *tls-1.0* TLS 1.0. *tls-1.1* TLS 1.1. *tls-1.2* TLS 1.2. *tls-1.3* TLS 1.3. *client* Use same value as client configuration.		
ssl-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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Send empty fragments. *disable* / Do not send empty fragments.		
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-
	Option / **Description** *disable* / Disable. *enable* / Enable.		
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-
	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-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-
	Option / **Description** *disable* / Do not keep session states. *time* / Expire session states after this many minutes. *count* / Expire session states when this maximum is reached. *both* / Expire session states based on time or count, whichever occurs first.		
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000

Parameter	Description	Type	Size
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-

Option	Description
disable	Do not keep session states.
time	Expire session states after this many minutes.
count	Expire session states when this maximum is reached.
both	Expire session states based on time or count, whichever occurs first.

ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-

Option	Description
enable	Enable HTTP location conversion.
disable	Disable HTTP location conversion.

ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-

Option	Description
enable	Match HTTP host in response header.
disable	Do not match HTTP host.

ssl-hpkp	Enable/disable including HPKP header in response.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Do not add a HPKP header to each HTTP response. *enable* Add a HPKP header to each a HTTP response. *report-only* Add a HPKP Report-Only header to each HTTP response.		
ssl-hpkp-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
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	-
	Option **Description** *disable* HPKP header does not apply to subdomains. *enable* HPKP header applies to subdomains.		
ssl-hsts	Enable/disable including HSTS header in response.	option	-
	Option **Description** *disable* Do not add a HSTS header to each a HTTP response. *enable* Add a HSTS header to each HTTP response.		
ssl-hsts-age	Number of seconds the client should honour the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* / HSTS header does not apply to subdomains. *enable* / 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

config realservers

Parameter	Description	Type	Size
ip	IPv6 address of the real server.	ipv6-address	Not Specified
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-
	Option / **Description** *active* / Server status active. *standby* / Server status standby. *disable* / Server status disable.		
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255
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
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable per server health check. *enable* — Enable per server health check. *vip* — 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
monitor	Name of the health check monitor to use when polling to determine a virtual server's connectivity status.	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
cipher	Cipher suite name.	option	-
	Option / **Description** *TLS-AES-128-GCM-SHA256* — Cipher suite TLS-AES-128-GCM-SHA256. *TLS-AES-256-GCM-SHA384* — Cipher suite TLS-AES-256-GCM-SHA384. *TLS-CHACHA20-POLY1305-SHA256* — Cipher suite TLS-CHACHA20-POLY1305-SHA256. *TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256* — Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		

Parameter	Description	Type	Size

Option	Description
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.

Parameter	Description	Type	Size

Option	Description
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.

Parameter	Description	Type	Size

Option	Description
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
TLS-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-RSA-WITH-RC4-128-MD5	Cipher suite TLS-RSA-WITH-RC4-128-MD5.
TLS-RSA-WITH-RC4-128-SHA	Cipher suite TLS-RSA-WITH-RC4-128-SHA.
TLS-DHE-RSA-WITH-DES-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.
TLS-DHE-DSS-WITH-DES-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.
TLS-RSA-WITH-DES-CBC-SHA	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.

versions	SSL/TLS versions that the cipher suite can be used with.	option	-

Parameter	Description	Type	Size

Option	Description
ssl-3.0	SSL 3.0.
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.
tls-1.2	TLS 1.2.
tls-1.3	TLS 1.3.

config ssl-server-cipher-suites

Parameter	Description	Type	Size
cipher	Cipher suite name.	option	-

Option	Description
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.

Parameter	Description	Type	Size

Option	Description
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

Option	Description
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.

Parameter	Description	Type	Size

Option	Description
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.

Parameter	Description	Type	Size

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

versions	SSL/TLS versions that the cipher suite can be used with.	option	-

Option	Description
ssl-3.0	SSL 3.0.
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.
tls-1.2	TLS 1.2.
tls-1.3	TLS 1.3.

config firewall vip64

Configure IPv6 to IPv4 virtual IPs.

```
config firewall vip64
   Description: Configure IPv6 to IPv4 virtual IPs.
   edit <name>
      set id {integer}
      set uuid {uuid}
      set comment {var-string}
      set type [static-nat|server-load-balance]
      set src-filter <range1>, <range2>, ...
      set extip {user}
      set mappedip {user}
      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|tcp|...]
      config realservers
         Description: Real servers.
         edit <id>
            set ip {ipv4-address-any}
            set port {integer}
            set status [active|standby|...]
            set weight {integer}
            set holddown-interval {integer}
            set healthcheck [disable|enable|...]
            set max-connections {integer}
            set monitor {string}
            set client-ip {user}
         next
      end
      set monitor <name1>, <name2>, ...
   next
end
```

config firewall vip64

Parameter	Description	Type	Size
id	Custom defined id.	integer	Minimum value: 0 Maximum value: 65535
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
type	VIP type: static NAT or server load balance.	option	-

Option	Description
static-nat	Static NAT.
server-load-balance	Server load balance.

Parameter	Description	Type	Size
src-filter <range>	Source IP6 filter (x:x:x:x:x:x:x:x/x). Src-filter range.	string	Maximum length: 79
extip	Start-external-IP [-end-external-IP].	user	Not Specified
mappedip	Start-mapped-IP [-end-mapped-IP].	user	Not Specified
arp-reply	Enable ARP reply.	option	-

Option	Description
disable	Disable arp reply.
enable	Enable arp reply.

Parameter	Description	Type	Size
portforward	Enable port forwarding.	option	-

Option	Description
disable	Disable port forwarding.
enable	Enable port forwarding.

Parameter	Description	Type	Size
protocol	Mapped port protocol.	option	-

Option	Description
tcp	TCP.
udp	UDP.

Parameter	Description	Type	Size
extport	External service port.	user	Not Specified
mappedport	Mapped service port.	user	Not Specified
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
ldb-method	Load balance method.	option	-

Parameter	Description	Type	Size
	Option / **Description** *static* — Distribute sessions based on source IP. *round-robin* — Distribute sessions based round robin order. *weighted* — Distribute sessions based on weight. *least-session* — Distribute sessions to the server with the lowest session count. *least-rtt* — Distribute sessions to the server with the lowest Round-Trip-Time. *first-alive* — Distribute sessions to the first server that is alive.		
server-type	Server type.	option	-
	Option / **Description** *http* — HTTP *tcp* — TCP *udp* — UDP *ip* — IP		
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79

config realservers

Parameter	Description	Type	Size
ip	Mapped server IP.	ipv4-address-any	Not Specified
port	Mapped server port.	integer	Minimum value: 1 Maximum value: 65535
status	Server administrative status.	option	-
	Option / **Description** *active* — Server status active. *standby* — Server status standby. *disable* — Server status disable.		

Parameter	Description	Type	Size
weight	weight	integer	Minimum value: 1 Maximum value: 255
holddown-interval	Hold down interval.	integer	Minimum value: 30 Maximum value: 65535
healthcheck	Per server health check.	option	-

Option	Description
disable	Disable per server health check.
enable	Enable per server health check.
vip	Use health check defined in VIP.

max-connections	Maximum number of connections allowed to server.	integer	Minimum value: 0 Maximum value: 2147483647
monitor	Health monitors.	string	Maximum length: 79
client-ip	Restrict server to a client IP in this range.	user	Not Specified

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
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
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
comments	Comment.	var-string	Maximum length: 255
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79

config firewall vipgrp46

Configure IPv4 to IPv6 virtual IP groups.

```
config firewall vipgrp46
   Description: Configure IPv4 to IPv6 virtual IP groups.
   edit <name>
      set uuid {uuid}
      set color {integer}
      set comments {var-string}
      set member <name1>, <name2>, ...
   next
end
```

config firewall vipgrp46

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32
comments	Comment.	var-string	Maximum length: 255

Parameter	Description	Type	Size
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP46 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
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32
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 vipgrp64

Configure IPv6 to IPv4 virtual IP groups.

```
config firewall vipgrp64
   Description: Configure IPv6 to IPv4 virtual IP groups.
   edit <name>
      set uuid {uuid}
      set color {integer}
      set comments {var-string}
      set member <name1>, <name2>, ...
   next
```

```
end
```

config firewall vipgrp64

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
color	Integer value to determine the color of the icon in the GUI .	integer	Minimum value: 0 Maximum value: 32
comments	Comment.	var-string	Maximum length: 255
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP64 name.	string	Maximum length: 79

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
bindthroughfw	Enable/disable use of IP/MAC binding to filter packets that would normally go through the firewall.	option	-

Option	Description
enable	Enable IP/MAC binding for packets that would normally go through the firewall.
disable	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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable IP/MAC binding for packets that would normally go to the firewall. *disable* — 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	-
	Option / **Description** *allow* — Allow packets from MAC addresses not in the IP/MAC list. *block* — 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
ip	IPv4 address portion of the pair (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
mac	MAC address portion of the pair (format: xx:xx:xx:xx:xx:xx in hexidecimal).	mac-address	Not Specified
name	Name of the pair .	string	Maximum length: 35
status	Enable/disable this IP-mac binding pair.	option	-
	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 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 fortinet-bar [enable|disable]
         set fortinet-bar-port {integer}
         set streaming-content-bypass [enable|disable]
         set switching-protocols [bypass|block]
         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 scan-bzip2 [enable|disable]
         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 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 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 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 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 scan-bzip2 [enable|disable]
      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 server-credential-type [none|credential-replication|...]
        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
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	-

Option	Description
disable	Disable logging for antivirus oversize file blocking.
enable	Enable logging for antivirus oversize file blocking.

switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable logging for HTTP/HTTPS switching protocols. *enable* — Enable logging for HTTP/HTTPS switching protocols.		
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-
	Option / **Description** *enable* — Enable inspection of RPC over HTTP. *disable* — Disable inspection of RPC over HTTP.		

config http

Parameter	Description	Type	Size
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	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
options	One or more options that can be applied to the session.	option	-
	Option / **Description** *clientcomfort* — Prevent client timeout. *servercomfort* — Prevent server timeout. *oversize* — Block oversized file/email. *chunkedbypass* — Bypass chunked transfer encoded sites.		

Parameter	Description	Type	Size
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
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535
range-block	Enable/disable blocking of partial downloads.	option	-

Option	Description
disable	Disable blocking of partial downloads.
enable	Enable blocking of partial downloads.

strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-

Option	Description
disable	Disable changing of HTTP X-Forwarded-For header.
enable	Enable replacement of X-Forwarded-For value with 1.1.1.1.

post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-

Option	Description
jisx0201	Japanese Industrial Standard 0201.
jisx0208	Japanese Industrial Standard 0208.
jisx0212	Japanese Industrial Standard 0212.
gb2312	Guojia Biaozhun 2312 (simplified Chinese).
ksc5601-ex	Wansung Korean standard 5601.
euc-jp	Extended Unicode Japanese.
sjis	Shift Japanese Industrial Standard.
iso2022-jp	ISO 2022 Japanese.
iso2022-jp-1	ISO 2022-1 Japanese.
iso2022-jp-2	ISO 2022-2 Japanese.
euc-cn	Extended Unicode Chinese.

Parameter	Description	Type	Size
	Option / **Description** *ces-gbk* — Extended GB2312 (simplified Chinese). *hz* — Hanzi simplified Chinese. *ces-big5* — Big-5 traditional Chinese. *euc-kr* — Extended Unicode Korean. *iso2022-jp-3* — ISO 2022-3 Japanese. *iso8859-1* — ISO 8859 Part 1 (Western European). *tis620* — Thai Industrial Standard 620. *cp874* — Code Page 874 (Thai). *cp1252* — Code Page 1252 (Western European Latin). *cp1251* — Code Page 1251 (Cyrillic).		
fortinet-bar	Enable/disable Fortinet bar on HTML content.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
fortinet-bar-port	Port for use by Fortinet Bar .	integer	Minimum value: 1 Maximum value: 65535
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-
	Option / **Description** *bypass* — Bypass connections when switching protocols. *block* — Block connections when switching protocols.		

Parameter	Description	Type	Size
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned .	integer	Minimum value: 0 Maximum value: 4294967295
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

block-page-status-code	Code number returned for blocked HTTP pages .	integer	Minimum value: 100 Maximum value: 599
retry-count	Number of attempts to retry HTTP connection .	integer	Minimum value: 0 Maximum value: 100
tcp-window-type	Specify type of TCP window to use for this protocol.	option	-

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, within limits.

Parameter	Description	Type	Size
tcp-window-minimum	Minimum dynamic TCP window size .	integer	Minimum value: 65536 Maximum value: 1048576
tcp-window-maximum	Maximum dynamic TCP window size .	integer	Minimum value: 1048576 Maximum value: 33554432
tcp-window-size	Set TCP static window size .	integer	Minimum value: 65536 Maximum value: 33554432
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-

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 ftp

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
options	One or more options that can be applied to the session.	option	-
	Option / **Description** *clientcomfort* / Prevent client timeout. *oversize* / Block oversized file/email. *splice* / Enable splice mode. *bypass-rest-command* / Bypass REST command. *bypass-mode-command* / 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
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-
	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
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	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
options	One or more options that can be applied to the session.	option	-
	Option / **Description** *fragmail* / Pass fragmented email. *oversize* / Block oversized file/email.		

Parameter	Description	Type	Size
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-

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 mapi

Parameter	Description	Type	Size
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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
options	One or more options that can be applied to the session.	option	-
	Option / **Description** *fragmail* — Pass fragmented email. *oversize* — Block oversized file/email.		
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		

** Values may differ between models.

config pop3

Parameter	Description	Type	Size
ports	Ports to scan for content .	integer	Minimum value: 1 Maximum value: 65535

Parameter	Description	Type	Size
status	Enable/disable the active status of scanning for this protocol.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
options	One or more options that can be applied to the session.	option	-

Option	Description
fragmail	Pass fragmented email.
oversize	Block oversized file/email.

Parameter	Description	Type	Size
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-

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 smtp

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

options	One or more options that can be applied to the session.	option	-

Option	Description
fragmail	Pass fragmented email.
oversize	Block oversized file/email.
splice	Enable splice mode.

Parameter	Description	Type	Size
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

server-busy	Enable/disable SMTP server busy when server not available.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-

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 nntp

Parameter	Description	Type	Size
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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
options	One or more options that can be applied to the session.	option	-
	Option **Description** *oversize* Block oversized file/email. *splice* Enable splice mode.		
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

** Values may differ between models.

config ssh

Parameter	Description	Type	Size
options	One or more options that can be applied to the session. **Option** **Description** *oversize* Block oversized file/email. *clientcomfort* Prevent client timeout. *servercomfort* Prevent server timeout.	option	-
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
comfort-amount	Amount of data to send in a transmission for client comforting .	integer	Minimum value: 1 Maximum value: 65535
oversize-limit	Maximum in-memory file size that can be scanned .	integer	Minimum value: 1 Maximum value: 186 **
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned .	integer	Minimum value: 0 Maximum value: 186 **
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned .	integer	Minimum value: 2 Maximum value: 100
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

** Values may differ between models.

config dns

Parameter	Description	Type	Size
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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

config cifs

Parameter	Description	Type	Size
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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
server-credential-type	CIFS server credential type.	option	-
	Option **Description** *none* Credential derivation not set.		

Parameter	Description	Type	Size
	Option / **Description** *credential-replication* — Credential derived using Replication account on Domain Controller. *credential-keytab* — Credential derived using server keytab.		

config server-keytab

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

config mail-signature

Parameter	Description	Type	Size
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiGate. **Option** / **Description** *disable* — Disable mail signature. *enable* — Enable mail signature.	option	-
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-cert-request [bypass|inspect|...]
         set unsupported-ssl [bypass|inspect|...]
         set invalid-server-cert [allow|block]
         set untrusted-server-cert [allow|block|...]
         set sni-server-cert-check [enable|strict|...]
      end
      config https
```

```
    Description: Configure HTTPS options.
    set ports {integer}
    set status [disable|certificate-inspection|...]
    set client-cert-request [bypass|inspect|...]
    set unsupported-ssl [bypass|inspect|...]
    set invalid-server-cert [allow|block]
    set untrusted-server-cert [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ftps
    Description: Configure FTPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set client-cert-request [bypass|inspect|...]
    set unsupported-ssl [bypass|inspect|...]
    set invalid-server-cert [allow|block]
    set untrusted-server-cert [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 client-cert-request [bypass|inspect|...]
    set unsupported-ssl [bypass|inspect|...]
    set invalid-server-cert [allow|block]
    set untrusted-server-cert [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 client-cert-request [bypass|inspect|...]
    set unsupported-ssl [bypass|inspect|...]
    set invalid-server-cert [allow|block]
    set untrusted-server-cert [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 client-cert-request [bypass|inspect|...]
    set unsupported-ssl [bypass|inspect|...]
    set invalid-server-cert [allow|block]
    set untrusted-server-cert [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 unsupported-version [bypass|block]
    set ssh-tun-policy-check [disable|enable]
    set ssh-algorithm [compatible|high-encryption]
```

```
      end
      set whitelist [enable|disable]
      set block-blacklisted-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 {string}
      config ssl-server
         Description: SSL servers.
         edit <id>
            set ip {ipv4-address-any}
            set https-client-cert-request [bypass|inspect|...]
            set smtps-client-cert-request [bypass|inspect|...]
            set pop3s-client-cert-request [bypass|inspect|...]
            set imaps-client-cert-request [bypass|inspect|...]
            set ftps-client-cert-request [bypass|inspect|...]
            set ssl-other-client-cert-request [bypass|inspect|...]
         next
      end
      set ssl-anomalies-log [disable|enable]
      set ssl-exemptions-log [disable|enable]
      set rpc-over-https [enable|disable]
      set mapi-over-https [enable|disable]
   next
end
```

config firewall ssl-ssh-profile

Parameter	Description	Type	Size
comment	Optional comments.	var-string	Maximum length: 255
whitelist	Enable/disable exempting servers by FortiGuard whitelist.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
block-blacklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blacklist.	option	-

Option	Description
disable	Disable FortiGuard certificate blacklist.
enable	Enable FortiGuard certificate blacklist.

Parameter	Description	Type	Size
server-cert-mode	Re-sign or replace the server's certificate.	option	-

Option	Description
re-sign	Multiple clients connecting to multiple servers.
replace	Protect an SSL server.

Parameter	Description	Type	Size
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-

Option	Description
disable	Don't use SSL server configuration.
enable	Use SSL server configuration.

Parameter	Description	Type	Size
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35
server-cert	Certificate used by SSL Inspection to replace server certificate.	string	Maximum length: 35
ssl-anomalies-log	Enable/disable logging SSL anomalies.	option	-

Option	Description
disable	Disable logging SSL anomalies.
enable	Enable logging SSL anomalies.

Parameter	Description	Type	Size
ssl-exemptions-log	Enable/disable logging SSL exemptions.	option	-

Option	Description
disable	Disable logging SSL exemptions.
enable	Enable logging SSL exemptions.

Parameter	Description	Type	Size
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-

Option	Description
enable	Enable inspection of RPC over HTTPS.
disable	Disable inspection of RPC over HTTPS.

Parameter	Description	Type	Size
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-

Option	Description
enable	Enable inspection of MAPI over HTTPS.
disable	Disable inspection of MAPI over HTTPS.

config ssl

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

Option	Description
disable	Disable.
certificate-inspection	Inspect SSL handshake only.
deep-inspection	Full SSL inspection.

Parameter	Description	Type	Size
client-cert-request	Action based on client certificate request.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-

Option	Description
allow	Allow the invalid server certificate.
block	Block the connection when an invalid server certificate is detected.

Parameter	Description	Type	Size
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-

Option	Description
allow	Allow the untrusted server certificate.
block	Block the connection when an untrusted server certificate is detected.
ignore	Always take the server certificate as trusted.

Parameter	Description	Type	Size
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-

Option	Description
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

config https

Parameter	Description	Type	Size
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535
status	Configure protocol inspection status.	option	-

Option	Description
disable	Disable.

Parameter	Description	Type	Size
	Option / **Description** *certificate-inspection* — Inspect SSL handshake only. *deep-inspection* — Full SSL inspection.		
client-cert-request	Action based on client certificate request.	option	-
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.		
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.		
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-
	Option / **Description** *allow* — Allow the invalid server certificate. *block* — Block the connection when an invalid server certificate is detected.		
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-
	Option / **Description** *allow* — Allow the untrusted server certificate. *block* — Block the connection when an untrusted server certificate is detected. *ignore* — Always take 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	-

Parameter	Description	Type	Size
	Option **Description** *enable* Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

config ftps

Parameter	Description	Type	Size
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535
status	Configure protocol inspection status.	option	-
	Option **Description** *disable* Disable. *deep-inspection* Full SSL inspection.		
client-cert-request	Action based on client certificate request.	option	-
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.		
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.		

Parameter	Description	Type	Size
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-

Option	Description
allow	Allow the invalid server certificate.
block	Block the connection when an invalid server certificate is detected.

Parameter	Description	Type	Size
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-

Option	Description
allow	Allow the untrusted server certificate.
block	Block the connection when an untrusted server certificate is detected.
ignore	Always take the server certificate as trusted.

Parameter	Description	Type	Size
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-

Option	Description
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

config imaps

Parameter	Description	Type	Size
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535
status	Configure protocol inspection status.	option	-

Option	Description
disable	Disable.
deep-inspection	Full SSL inspection.

Parameter	Description	Type	Size
client-cert-request	Action based on client certificate request.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-

Option	Description
allow	Allow the invalid server certificate.
block	Block the connection when an invalid server certificate is detected.

Parameter	Description	Type	Size
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-

Option	Description
allow	Allow the untrusted server certificate.
block	Block the connection when an untrusted server certificate is detected.
ignore	Always take the server certificate as trusted.

Parameter	Description	Type	Size
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-

Option	Description
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.

Parameter	Description	Type	Size
	Option / **Description** *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

config pop3s

Parameter	Description	Type	Size
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535
status	Configure protocol inspection status.	option	-
	Option / **Description** *disable* — Disable. *deep-inspection* — Full SSL inspection.		
client-cert-request	Action based on client certificate request.	option	-
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.		
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.		
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-

Parameter	Description	Type	Size
	Option / **Description** *allow* — Allow the invalid server certificate. *block* — Block the connection when an invalid server certificate is detected.		
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-
	Option / **Description** *allow* — Allow the untrusted server certificate. *block* — Block the connection when an untrusted server certificate is detected. *ignore* — Always take 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	-
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

config smtps

Parameter	Description	Type	Size
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535
status	Configure protocol inspection status.	option	-
	Option / **Description** *disable* — Disable. *deep-inspection* — Full SSL inspection.		
client-cert-request	Action based on client certificate request.	option	-

Parameter	Description	Type	Size
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.		
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.		
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-
	Option / **Description** *allow* — Allow the invalid server certificate. *block* — Block the connection when an invalid server certificate is detected.		
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-
	Option / **Description** *allow* — Allow the untrusted server certificate. *block* — Block the connection when an untrusted server certificate is detected. *ignore* — Always take 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	-
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

config ssh

Parameter	Description	Type	Size
ports	Ports to use for scanning .	integer	Minimum value: 1 Maximum value: 65535
status	Configure protocol inspection status.	option	-

Option	Description
disable	Disable.
deep-inspection	Full SSL inspection.

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

Option	Description
disable	Disable.
deep-inspection	Full SSL inspection.

Parameter	Description	Type	Size
unsupported-version	Action based on SSH version being unsupported.	option	-

Option	Description
bypass	Bypass the session.
block	Block the session.

Parameter	Description	Type	Size
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-

Option	Description
disable	Disable SSH tunnel policy check.
enable	Enable SSH tunnel policy check.

Parameter	Description	Type	Size
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-

Option	Description
compatible	Allow a broader set of encryption algorithms for best compatibility.
high-encryption	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.

config ssl-exempt

Parameter	Description	Type	Size
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-

Option	Description
fortiguard-category	FortiGuard category.
address	Firewall IPv4 address.
address6	Firewall IPv6 address.
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.
regex	Regular expression FQDN.

fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255
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
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified
https-client-cert-request	Action based on client certificate request during the HTTPS handshake.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
smtps-client-cert-request	Action based on client certificate request during the SMTPS handshake.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
pop3s-client-cert-request	Action based on client certificate request during the POP3S handshake.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
imaps-client-cert-request	Action based on client certificate request during the IMAPS handshake.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
ftps-client-cert-request	Action based on client certificate request during the FTPS handshake.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size
ssl-other-client-cert-request	Action based on client certificate request during an SSL protocol handshake.	option	-

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	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 ips-sensor {string}
      set application-list {string}
      set voip-profile {string}
      set icap-profile {string}
      set cifs-profile {string}
      set waf-profile {string}
      set ssh-filter-profile {string}
   next
end
```

config firewall profile-group

Parameter	Description	Type	Size
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
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
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35

Parameter	Description	Type	Size
application-list	Name of an existing Application list.	string	Maximum length: 35
voip-profile	Name of an existing VoIP 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
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
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified

Parameter	Description	Type	Size
port	Server service port .	integer	Minimum value: 1 Maximum value: 65535
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-

Option	Description
half	Client to FortiGate SSL.
full	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	-

Option	Description
enable	Add X-Forwarded-Proto header.
disable	Do not add X-Forwarded-Proto header.

mapped-port	Mapped server service port .	integer	Minimum value: 1 Maximum value: 65535
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-

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	-

Option	Description
high	High encryption. Allow only AES and ChaCha
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.

Parameter	Description	Type	Size
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-

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.

Parameter	Description	Type	Size
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-

Option	Description
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.
tls-1.2	TLS 1.2.

Parameter	Description	Type	Size
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-

Option	Description
tls-1.0	TLS 1.0.
tls-1.1	TLS 1.1.
tls-1.2	TLS 1.2.

Parameter	Description	Type	Size
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV.	option	-

Option	Description
enable	Send empty fragments.
disable	Do not send empty fragments.

Parameter	Description	Type	Size
url-rewrite	Enable/disable rewriting the URL.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

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
comments	Comments.	string	Maximum length: 127

config rule

Parameter	Description	Type	Size
gateway	IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx , Default: 0.0.0.0).	ipv4-address	Not Specified
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
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 consolidated policy

Configure consolidated IPv4/IPv6 policies.

```
config firewall consolidated policy
   Description: Configure consolidated IPv4/IPv6 policies.
   edit <policyid>
      set status [enable|disable]
      set name {string}
      set uuid {uuid}
      set srcintf <name1>, <name2>, ...
      set dstintf <name1>, <name2>, ...
      set srcaddr4 <name1>, <name2>, ...
      set dstaddr4 <name1>, <name2>, ...
      set srcaddr6 <name1>, <name2>, ...
      set dstaddr6 <name1>, <name2>, ...
      set srcaddr-negate [enable|disable]
      set dstaddr-negate [enable|disable]
      set service-negate [enable|disable]
      set internet-service [enable|disable]
      set internet-service-id <id1>, <id2>, ...
      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-id <id1>, <id2>, ...
      set internet-service-src-group <name1>, <name2>, ...
      set internet-service-src-custom <name1>, <name2>, ...
      set internet-service-src-custom-group <name1>, <name2>, ...
      set internet-service-negate [enable|disable]
      set internet-service-src-negate [enable|disable]
      set action [accept|deny|...]
      set schedule {string}
      set service <name1>, <name2>, ...
      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 ips-sensor {string}
      set application-list {string}
      set voip-profile {string}
      set icap-profile {string}
      set cifs-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 groups <name1>, <name2>, ...
      set users <name1>, <name2>, ...
      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 webproxy-forward-server {string}
      set traffic-shaper {string}
      set traffic-shaper-reverse {string}
      set per-ip-shaper {string}
      set nat [enable|disable]
      set fixedport [enable|disable]
      set ippool [enable|disable]
      set poolname4 <name1>, <name2>, ...
      set poolname6 <name1>, <name2>, ...
      set session-ttl {integer}
      set comments {var-string}
      set vpntunnel {string}
      set inbound [enable|disable]
      set outbound [enable|disable]
      set captive-portal-exempt [enable|disable]
      set fsso-groups <name1>, <name2>, ...
   next
end
```

config firewall consolidated policy

Parameter	Description	Type	Size
status	Enable or disable this policy.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
name	Policy name.	string	Maximum length: 35
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79
srcaddr4 <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79
dstaddr4 <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 specifies what the source address must NOT be.	option	-
	Option **Description** *enable* Enable source address negate. *disable* Disable source address negate.		
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-
	Option **Description** *enable* Enable destination address negate. *disable* Disable destination address negate.		

Parameter	Description	Type	Size
service-negate	When enabled service specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated service match.
disable	Disable negated service match.

Parameter	Description	Type	Size
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-

Option	Description
enable	Enable use of Internet Services in policy.
disable	Disable use of Internet Services in policy.

Parameter	Description	Type	Size
internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
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	-

Option	Description
enable	Enable use of Internet Services source in policy.
disable	Disable use of Internet Services source in policy.

Parameter	Description	Type	Size
internet-service-src-id <id>	Internet Service source ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
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
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated Internet Service match.
disable	Disable negated Internet Service match.

internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated Internet Service source match.
disable	Disable negated Internet Service source match.

action	Policy action (allow/deny/ipsec).	option	-

Option	Description
accept	Allows session that match the firewall policy.
deny	Blocks sessions that match the firewall policy.
ipsec	Firewall policy becomes a policy-based IPsec VPN policy.

schedule	Schedule name.	string	Maximum length: 35
service <name>	Service and service group names. Service name.	string	Maximum length: 79
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-
	Option / **Description** *proxy* / Proxy based inspection. *flow* / Flow based inspection.		
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-
	Option / **Description** *enable* / Enable HTTP(S) policy redirect. *disable* / Disable HTTP(S) policy redirect.		
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-
	Option / **Description** *enable* / Enable SSH policy redirect. *disable* / 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	-
	Option / **Description** *single* / Do not allow security profile groups. *group* / 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

Parameter	Description	Type	Size
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
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
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
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35
cifs-profile	Name of an existing CIFS 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	-

Option	Description
all	Log all sessions accepted or denied by this policy.
utm	Log traffic that has a security profile applied to it.
disable	Disable all logging for this policy.

logtraffic-start	Record logs when a session starts.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
auto-asic-offload	Enable/disable policy traffic ASIC offloading.	option	-
	Option **Description** *enable* Enable auto ASIC offloading. *disable* Disable ASIC offloading.		
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. User name.	string	Maximum length: 79
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-
	Option **Description** *enable* Enable forward (original) traffic DiffServ. *disable* Disable forward (original) traffic DiffServ.		
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-
	Option **Description** *enable* Enable reverse (reply) traffic DiffServ. *disable* Disable 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

Parameter	Description	Type	Size
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ippool	Enable to use IP Pools for source NAT.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
poolname4 <name>	IPv4 pool names. IPv4 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 .	integer	Minimum value: 300 Maximum value: 2764800

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 1023
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

captive-portal-exempt	Enable exemption of some users from the captive portal.	option	-

Option	Description
enable	Enable exemption of captive portal.
disable	Disable exemption of captive portal.

fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511

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 srcaddr4 <name1>, <name2>, ...
      set dstaddr4 <name1>, <name2>, ...
      set srcaddr6 <name1>, <name2>, ...
      set dstaddr6 <name1>, <name2>, ...
      set internet-service [enable|disable]
      set internet-service-id <id1>, <id2>, ...
```

```
    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-id <id1>, <id2>, ...
    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 logtraffic-start [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 ips-sensor {string}
    set application-list {string}
    set voip-profile {string}
    set icap-profile {string}
    set cifs-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 fsso-groups <name1>, <name2>, ...
  next
end
```

config firewall security-policy

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
name	Policy name.	string	Maximum length: 35

Parameter	Description	Type	Size
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
srcaddr4 <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79
dstaddr4 <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
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-

Option	Description
enable	Enable use of Internet Services in policy.
disable	Disable use of Internet Services in policy.

internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated Internet Service match.
disable	Disable negated Internet Service match.

Parameter	Description	Type	Size
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	-
	Option / **Description** *enable* — Enable use of Internet Services source in policy. *disable* — Disable use of Internet Services source in policy.		
internet-service-src-id <id>	Internet Service source ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-
	Option / **Description** *enable* — Enable negated Internet Service source match. *disable* — 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

Parameter	Description	Type	Size
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable negated service match.
disable	Disable negated service match.

Parameter	Description	Type	Size
action	Policy action (accept/deny).	option	-

Option	Description
accept	Allows session that match the firewall policy.
deny	Blocks sessions that match the firewall policy.

Parameter	Description	Type	Size
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-

Option	Description
disable	Disable deny-packet sending.
enable	Enable deny-packet sending.

Parameter	Description	Type	Size
schedule	Schedule name.	string	Maximum length: 35
status	Enable or disable this policy.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-

Parameter	Description	Type	Size
	Option / **Description** *all* — Log all sessions accepted or denied by this policy. *utm* — Log traffic that has a security profile applied to it. *disable* — Disable all logging for this policy.		
logtraffic-start	Record logs when a session starts.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-
	Option / **Description** *single* — Do not allow security profile groups. *group* — 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
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
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
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
voip-profile	Name of an existing VoIP 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
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
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511

config firewall policy

Configure IPv4 policies.

```
config firewall policy
   Description: Configure IPv4 policies.
   edit <policyid>
      set name {string}
```

```
set uuid {uuid}
set srcintf <name1>, <name2>, ...
set dstintf <name1>, <name2>, ...
set srcaddr <name1>, <name2>, ...
set dstaddr <name1>, <name2>, ...
set internet-service [enable|disable]
set internet-service-id <id1>, <id2>, ...
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-id <id1>, <id2>, ...
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 rtp-nat [disable|enable]
set rtp-addr <name1>, <name2>, ...
set action [accept|deny|...]
set send-deny-packet [disable|enable]
set firewall-session-dirty [check-all|check-new]
set status [enable|disable]
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 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 ips-sensor {string}
set application-list {string}
set voip-profile {string}
set icap-profile {string}
set cifs-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 application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set url-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
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 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 fsso [enable|disable]
set wsso [enable|disable]
set rsso [enable|disable]
set fsso-agent-for-ntlm {string}
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set fsso-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 {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 ssl-mirror [enable|disable]
    set ssl-mirror-intf <name1>, <name2>, ...
    set dsri [enable|disable]
    set radius-mac-auth-bypass [enable|disable]
    set delay-tcp-npu-session [enable|disable]
    set vlan-filter {user}
  next
end
```

config firewall policy

Parameter	Description	Type	Size
name	Policy name.	string	Maximum length: 35
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
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 address and address group names. Address name.	string	Maximum length: 79
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-

Option	Description
enable	Enable use of Internet Services in policy.
disable	Disable use of Internet Services in policy.

internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable use of Internet Services source in policy.
disable	Disable use of Internet Services source in policy.

internet-service-src-id <id>	Internet Service source ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
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
reputation-direction	Direction of the initial traffic for reputation to take effect.	option	-

Option	Description
source	Check reputation for source address.
destination	Check reputation for destination address.

Parameter	Description	Type	Size
rtp-nat	Enable Real Time Protocol (RTP) NAT.	option	-

Option	Description
disable	Disable setting.
enable	Enable setting.

Parameter	Description	Type	Size
rtp-addr <name>	Address names if this is an RTP NAT policy. Address name.	string	Maximum length: 79
action	Policy action (allow/deny/ipsec).	option	-

Option	Description
accept	Allows session that match the firewall policy.
deny	Blocks sessions that match the firewall policy.
ipsec	Firewall policy becomes a policy-based IPsec VPN policy.

Parameter	Description	Type	Size
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-

Option	Description
disable	Disable deny-packet sending.
enable	Enable deny-packet sending.

Parameter	Description	Type	Size
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-

Option	Description
check-all	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.
check-new	Continue to allow sessions already accepted by this policy.

Parameter	Description	Type	Size
status	Enable or disable this policy.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
schedule	Schedule name.	string	Maximum length: 35

Parameter	Description	Type	Size
schedule-timeout	Enable to force current sessions to end when the schedule object times out. Disable allows them to end from inactivity.	option	-

Option	Description
enable	Enable schedule timeout.
disable	Disable schedule timeout.

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	-

Option	Description
enable	Enable TOS match negate.
disable	Disable TOS match negate.

anti-replay	Enable/disable anti-replay check.	option	-

Option	Description
enable	Enable anti-replay check.
disable	Disable anti-replay check.

tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-

Option	Description
all	Enable TCP session without SYN.
data-only	Enable TCP session data only.
disable	Disable TCP session without SYN.

geoip-anycast	Enable/disable recognition of anycast IP addresses using the geography IP database.	option	-

Option	Description
enable	Enable recognition of anycast IP addresses using the geography IP database.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable recognition of anycast IP addresses using the geography IP database.		
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-
	Option **Description** *proxy* Proxy based inspection. *flow* Flow based inspection.		
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-
	Option **Description** *enable* Enable HTTP(S) policy redirect. *disable* Disable HTTP(S) policy redirect.		
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-
	Option **Description** *enable* Enable SSH policy redirect. *disable* 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	-
	Option **Description** *single* Do not allow security profile groups. *group* Allow security profile groups.		

Parameter	Description	Type	Size
profile-group	Name of profile group.	string	Maximum length: 35
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
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
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
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35
cifs-profile	Name of an existing CIFS 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	-

Option	Description
all	Log all sessions accepted or denied by this policy.

Parameter	Description	Type	Size
	Option **Description** *utm* Log traffic that has a security profile applied to it. *disable* Disable all logging for this policy.		
logtraffic-start	Record logs when a session starts.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
auto-asic-offload	Enable/disable policy traffic ASIC offloading.	option	-
	Option **Description** *enable* Enable auto ASIC offloading. *disable* Disable ASIC offloading.		
np-acceleration *	Enable/disable UTM Network Processor acceleration.	option	-
	Option **Description** *enable* Enable UTM Network Processor acceleration. *disable* 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
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
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
nat	Enable/disable source NAT.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
permit-any-host	Accept UDP packets from any host.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
permit-stun-host	Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ippool	Enable to use IP Pools for source NAT.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
poolname <name>	IP Pool names. IP 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
vlan-cos-rev	VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
wccp	Enable/disable forwarding traffic matching this policy to a configured WCCP server.	option	-
	Option **Description** *enable* Enable WCCP setting. *disable* Disable WCCP setting.		
ntlm	Enable/disable NTLM authentication.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ntlm-guest	Enable/disable NTLM guest user access.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ntlm-enabled-browsers `<user-agent-string>`	HTTP-User-Agent value of supported browsers. User agent string.	string	Maximum length: 79
fsso	Enable/disable Fortinet Single Sign-On.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
wsso	Enable/disable WiFi Single Sign On (WSSO).	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

Parameter	Description	Type	Size
rsso	Enable/disable RADIUS single sign-on (RSSO).	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
fsso-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
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511
auth-path	Enable/disable authentication-based routing.	option	-
	Option / **Description** *enable* — Enable authentication-based routing. *disable* — Disable authentication-based routing.		
disclaimer	Enable/disable user authentication disclaimer.	option	-
	Option / **Description** *enable* — Enable user authentication disclaimer. *disable* — Disable user authentication disclaimer.		
email-collect	Enable/disable email collection.	option	-
	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

Parameter	Description	Type	Size
match-vip	Enable to match packets that have had their destination addresses changed by a VIP.	option	-

Option	Description
enable	Match DNATed packet.
disable	Do not match DNATed packet.

Parameter	Description	Type	Size
match-vip-only	Enable/disable matching of only those packets that have had their destination addresses changed by a VIP.	option	-

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
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-

Option	Description
enable	Enable setting forward (original) traffic Diffserv.
disable	Disable setting forward (original) traffic Diffserv.

Parameter	Description	Type	Size
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-

Option	Description
enable	Enable setting reverse (reply) traffic DiffServ.
disable	Disable setting reverse (reply) traffic DiffServ.

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535
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.	string	Maximum length: 255
identity-based-route	Name of identity-based routing rule.	string	Maximum length: 35
block-notification	Enable/disable block notification.	option	-

Option	Description
enable	Enable setting.
disable	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 specifies what the source address must NOT be.	option	-

Option	Description
enable	Enable source address negate.
disable	Disable source address negate.

dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-

Option	Description
enable	Enable destination address negate.
disable	Disable destination address negate.

Parameter	Description	Type	Size
service-negate	When enabled service specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated service match.
disable	Disable negated service match.

Parameter	Description	Type	Size
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated Internet Service match.
disable	Disable negated Internet Service match.

Parameter	Description	Type	Size
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-

Option	Description
enable	Enable negated Internet Service source match.
disable	Disable negated Internet Service source match.

Parameter	Description	Type	Size
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-

Option	Description
enable	Enable sending of RST packet upon TCP session expiration.
disable	Disable sending of RST packet upon TCP session expiration.

Parameter	Description	Type	Size
captive-portal-exempt	Enable to exempt some users from the captive portal.	option	-

Option	Description
enable	Enable exemption of captive portal.
disable	Disable exemption of captive portal.

Parameter	Description	Type	Size
ssl-mirror	Enable to copy decrypted SSL traffic to a FortiGate interface (called SSL mirroring).	option	-

Option	Description
enable	Enable SSL mirror.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable SSL mirror.		
ssl-mirror-intf <name>	SSL mirror interface name. Mirror Interface name.	string	Maximum length: 79
dsri	Enable DSRI to ignore HTTP server responses.	option	-
	Option **Description** *enable* Enable DSRI. *disable* Disable DSRI.		
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	option	-
	Option **Description** *enable* Enable MAC authentication bypass. *disable* Disable MAC authentication bypass.		
delay-tcp-npu-session	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-
	Option **Description** *enable* Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake. *disable* Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.		
vlan-filter	Set VLAN filters.	user	Not Specified

* 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
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-id <id1>, <id2>, ...
      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-id <id1>, <id2>, ...
      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
name	Shaping policy name.	string	Maximum length: 35
comment	Comments.	var-string	Maximum length: 255
status	Enable/disable this traffic shaping policy.	option	-

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	-

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	-

Option	Description
enable	Enable use of Internet Service in shaping-policy.
disable	Disable use of Internet Service in shaping-policy.

internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
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	-

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-id <id>	Internet Service source ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
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

Parameter	Description	Type	Size
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
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	-

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

Parameter	Description	Type	Size
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-

Option	Description
enable	Enable setting forward (original) traffic DiffServ.
disable	Disable setting forward (original) traffic DiffServ.

diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-

Option	Description
enable	Enable setting reverse (reply) traffic DiffServ.
disable	Disable setting reverse (reply) traffic DiffServ.

diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified

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
comment	Comment.	var-string	Maximum length: 1023
type	Select shaping profile type: policing / queuing.	option	-

Option	Description
policing	Enable policing mode.
queuing	Enable queuing mode.

Parameter	Description	Type	Size
default-class-id	Default class ID to handle unclassified packets (including all local traffic).	integer	Minimum value: 0 Maximum value: 4294967295

config shaping-entries

Parameter	Description	Type	Size
class-id	Class ID.	integer	Minimum value: 0 Maximum value: 4294967295
priority	Priority.	option	-

Option	Description
top	Top priority.
critical	Critical priority.
high	High priority.
medium	Medium priority.
low	Low priority.

Parameter	Description	Type	Size
guaranteed-bandwidth-percentage	Guaranteed bandwith in percentage.	integer	Minimum value: 0 Maximum value: 100
maximum-bandwidth-percentage	Maximum bandwith in percentage.	integer	Minimum value: 1 Maximum value: 100
limit	Hard limit on the real queue size in packets.	integer	Minimum value: 5 Maximum value: 10000
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
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
red-probability	Maximum probability (in percentage) for RED marking.	integer	Minimum value: 0 Maximum value: 20
min	Average queue size in packets at which RED drop becomes a possibility.	integer	Minimum value: 3 Maximum value: 3000
max	Average queue size in packets at which RED drop probability is maximal.	integer	Minimum value: 3 Maximum value: 3000

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 ha-mgmt-intf-only [enable|disable]
      set intf {string}
      set srcaddr <name1>, <name2>, ...
      set dstaddr <name1>, <name2>, ...
      set action [accept|deny]
```

```
    set service <name1>, <name2>, ...
    set schedule {string}
    set status [enable|disable]
    set comments {var-string}
  next
end
```

config firewall local-in-policy

Parameter	Description	Type	Size
ha-mgmt-intf-only	Enable/disable dedicating the HA management interface only for local-in policy.	option	-
	Option / **Description** *enable* — Enable dedicating HA management interface only for local-in policy. *disable* — 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
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79
action	Action performed on traffic matching the policy .	option	-
	Option / **Description** *accept* — Allow traffic matching this policy. *deny* — Deny or block traffic matching this policy.		
service <name>	Service object from available options. Service name.	string	Maximum length: 79
schedule	Schedule object from available options.	string	Maximum length: 35
status	Enable/disable this local-in policy.	option	-
	Option / **Description** *enable* — Enable this local-in policy. *disable* — Disable this local-in policy.		
comments	Comment.	var-string	Maximum length: 1023

config firewall policy6

Configure IPv6 policies.

```
config firewall policy6
   Description: Configure IPv6 policies.
   edit <policyid>
      set name {string}
      set uuid {uuid}
      set srcintf <name1>, <name2>, ...
      set dstintf <name1>, <name2>, ...
      set srcaddr <name1>, <name2>, ...
      set dstaddr <name1>, <name2>, ...
      set action [accept|deny|...]
      set firewall-session-dirty [check-all|check-new]
      set status [enable|disable]
      set vlan-cos-fwd {integer}
      set vlan-cos-rev {integer}
      set schedule {string}
      set service <name1>, <name2>, ...
      set tos {user}
      set tos-mask {user}
      set tos-negate [enable|disable]
      set tcp-session-without-syn [all|data-only|...]
      set anti-replay [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 ips-sensor {string}
      set application-list {string}
      set voip-profile {string}
      set icap-profile {string}
      set cifs-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 application <id1>, <id2>, ...
      set app-category <id1>, <id2>, ...
      set url-category <id1>, <id2>, ...
```

```
    set app-group <name1>, <name2>, ...
    set nat [enable|disable]
    set fixedport [enable|disable]
    set ippool [enable|disable]
    set poolname <name1>, <name2>, ...
    set session-ttl {user}
    set inbound [enable|disable]
    set outbound [enable|disable]
    set natinbound [enable|disable]
    set natoutbound [enable|disable]
    set send-deny-packet [enable|disable]
    set vpntunnel {string}
    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 rsso [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 groups <name1>, <name2>, ...
    set users <name1>, <name2>, ...
    set timeout-send-rst [enable|disable]
    set ssl-mirror [enable|disable]
    set ssl-mirror-intf <name1>, <name2>, ...
    set dsri [enable|disable]
    set vlan-filter {user}
    set fsso-groups <name1>, <name2>, ...
  next
end
```

config firewall policy6

Parameter	Description	Type	Size
name	Policy name.	string	Maximum length: 35
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
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 address and address group names. Address name.	string	Maximum length: 79

Parameter	Description	Type	Size
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79
action	Policy action (allow/deny/ipsec).	option	-

Option	Description
accept	Allows session that match the firewall policy.
deny	Blocks sessions that match the firewall policy.
ipsec	Firewall policy becomes a policy-based IPsec VPN policy.

firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-

Option	Description
check-all	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.
check-new	Continue to allow sessions already accepted by this policy.

status	Enable or disable this policy.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

vlan-cos-fwd	VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest	integer	Minimum value: 0 Maximum value: 7
vlan-cos-rev	VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest	integer	Minimum value: 0 Maximum value: 7
schedule	Schedule name.	string	Maximum length: 35
service <name>	Service and service group names. Address 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	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable TOS match negate. *disable* Disable TOS match negate.		
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-
	Option **Description** *all* Enable TCP session without SYN. *data-only* Enable TCP session data only. *disable* Disable TCP session without SYN.		
anti-replay	Enable/disable anti-replay check.	option	-
	Option **Description** *enable* Enable anti-replay check. *disable* Disable anti-replay check.		
utm-status	Enable AV/web/ips protection profile.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-
	Option **Description** *proxy* Proxy based inspection. *flow* Flow based inspection.		
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-
	Option **Description** *enable* Enable HTTP(S) policy redirect. *disable* Disable HTTP(S) policy redirect.		
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable SSH policy redirect. *disable* / 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	-
	Option / **Description** *single* / Do not allow security profile groups. *group* / 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
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
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
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
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35

Parameter	Description	Type	Size
cifs-profile	Name of an existing CIFS 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	-

Option	Description
all	Log all sessions accepted or denied by this policy.
utm	Log traffic that has a security profile applied to it.
disable	Disable all logging for this policy.

logtraffic-start	Record logs when a session starts.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

auto-asic-offload	Enable/disable policy traffic ASIC offloading.	option	-

Option	Description
enable	Enable auto ASIC offloading.
disable	Disable ASIC offloading.

np-acceleration *	Enable/disable UTM Network Processor acceleration.	option	-

Option	Description
enable	Enable UTM Network Processor acceleration.
disable	Disable UTM Network Processor acceleration.

webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63
traffic-shaper	Reverse traffic shaper.	string	Maximum length: 35
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35

Parameter	Description	Type	Size
per-ip-shaper	Per-IP traffic shaper.	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
nat	Enable/disable source NAT.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

fixedport	Enable to prevent source NAT from changing a session's source port.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

ippool	Enable to use IP Pools for source NAT.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79

Parameter	Description	Type	Size
session-ttl	Session TTL in seconds for sessions accepted by this policy. 0 means use the system default session TTL.	user	Not Specified
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
send-deny-packet	Enable/disable return of deny-packet.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable forward (original) traffic DiffServ. *disable* Disable forward (original) traffic DiffServ.		
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-
	Option **Description** *enable* Enable reverse (reply) traffic DiffServ. *disable* Disable 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
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535
comments	Comment.	var-string	Maximum length: 1023
rsso	Enable/disable RADIUS single sign-on (RSSO).	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
custom-log-fields <field-id>	Log field index numbers to append custom log fields to log messages for this policy. Custom log field.	string	Maximum length: 35
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable source address negate. *disable* Disable destination address negate.		
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-
	Option **Description** *enable* Enable source address negate. *disable* Disable destination address negate.		
service-negate	When enabled service specifies what the service must NOT be.	option	-
	Option **Description** *enable* Enable negated service match. *disable* Disable negated service match.		
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
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-
	Option **Description** *enable* Send RST when session times out. *disable* Donot send RST when session times out.		
ssl-mirror	Enable to copy decrypted SSL traffic to a FortiGate interface (called SSL mirroring).	option	-
	Option **Description** *enable* Enable SSL mirror. *disable* Disable SSL mirror.		
ssl-mirror-intf <name>	SSL mirror interface name. Interface name.	string	Maximum length: 79

Parameter	Description	Type	Size
dsri	Enable DSRI to ignore HTTP server responses.	option	-
	Option / **Description** *enable* / Enable DSRI. *disable* / Disable DSRI.		
vlan-filter	Set VLAN filters.	user	Not Specified
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511

* This parameter may not exist in some models.

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 intf {string}
      set srcaddr <name1>, <name2>, ...
      set dstaddr <name1>, <name2>, ...
      set action [accept|deny]
      set service <name1>, <name2>, ...
      set schedule {string}
      set status [enable|disable]
      set comments {var-string}
   next
end
```

config firewall local-in-policy6

Parameter	Description	Type	Size
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
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79
action	Action performed on traffic matching the policy .	option	-

Parameter	Description	Type	Size
	Option / **Description** *accept* — Allow local-in traffic matching this policy. *deny* — 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
schedule	Schedule object from available options.	string	Maximum length: 35
status	Enable/disable this local-in policy.	option	-
	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
status	Enable/disable this TTL policy.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable this TTL policy. *disable* — Disable this TTL policy.		
action	Action to be performed on traffic matching this policy . **Option** / **Description** *accept* — Allow traffic matching this policy. *deny* — Deny or block traffic matching this policy.	option	-
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 policy64

Configure IPv6 to IPv4 policies.

```
config firewall policy64
   Description: Configure IPv6 to IPv4 policies.
   edit <policyid>
      set uuid {uuid}
      set srcintf {string}
      set dstintf {string}
      set srcaddr <name1>, <name2>, ...
      set dstaddr <name1>, <name2>, ...
      set action [accept|deny]
      set status [enable|disable]
      set schedule {string}
      set service <name1>, <name2>, ...
      set logtraffic [enable|disable]
      set logtraffic-start [enable|disable]
      set permit-any-host [enable|disable]
      set traffic-shaper {string}
      set traffic-shaper-reverse {string}
      set per-ip-shaper {string}
```

```
      set fixedport [enable|disable]
      set ippool [enable|disable]
      set poolname <name1>, <name2>, ...
      set tcp-mss-sender {integer}
      set tcp-mss-receiver {integer}
      set comments {var-string}
   next
end
```

config firewall policy64

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
srcintf	Source interface name.	string	Maximum length: 35
dstintf	Destination 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
action	Policy action.	option	-

Option	Description
accept	Action accept.
deny	Action deny.

status	Enable/disable policy status.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

schedule	Schedule name.	string	Maximum length: 35
service <name>	Service name. Address name.	string	Maximum length: 79
logtraffic	Enable/disable policy log traffic.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
logtraffic-start	Record logs when a session starts and ends.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
permit-any-host	Enable/disable permit any host in.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
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
fixedport	Enable/disable policy fixed port.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ippool	Enable/disable policy64 IP pool.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
poolname <name>	Policy IP pool names. IP pool name.	string	Maximum length: 79

Parameter	Description	Type	Size
tcp-mss-sender	TCP MSS value of sender.	integer	Minimum value: 0 Maximum value: 65535
tcp-mss-receiver	TCP MSS value of receiver.	integer	Minimum value: 0 Maximum value: 65535
comments	Comment.	var-string	Maximum length: 1023

config firewall policy46

Configure IPv4 to IPv6 policies.

```
config firewall policy46
   Description: Configure IPv4 to IPv6 policies.
   edit <policyid>
      set permit-any-host [enable|disable]
      set uuid {uuid}
      set srcintf {string}
      set dstintf {string}
      set srcaddr <name1>, <name2>, ...
      set dstaddr <name1>, <name2>, ...
      set action [accept|deny]
      set status [enable|disable]
      set schedule {string}
      set service <name1>, <name2>, ...
      set logtraffic [enable|disable]
      set logtraffic-start [enable|disable]
      set traffic-shaper {string}
      set traffic-shaper-reverse {string}
      set per-ip-shaper {string}
      set fixedport [enable|disable]
      set tcp-mss-sender {integer}
      set tcp-mss-receiver {integer}
      set comments {var-string}
      set ippool [enable|disable]
      set poolname <name1>, <name2>, ...
   next
end
```

config firewall policy46

Parameter	Description	Type	Size
permit-any-host	Enable/disable allowing any host.	option	-

Option	Description
enable	Allow any host.
disable	Do not allow any host.

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
srcintf	Source interface name.	string	Maximum length: 35
dstintf	Destination interface name.	string	Maximum length: 35
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79
action	Accept or deny traffic matching the policy.	option	-

Option	Description
accept	Accept matching traffic.
deny	Deny matching traffic.

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

Option	Description
enable	Enable this policy.
disable	Disable this policy.

Parameter	Description	Type	Size
schedule	Schedule name.	string	Maximum length: 35
service <name>	Service name. Service name.	string	Maximum length: 79
logtraffic	Enable/disable traffic logging for this policy.	option	-

Option	Description
enable	Enable traffic logging.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable traffic logging.		
logtraffic-start	Record logs when a session starts and ends.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
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
fixedport	Enable/disable fixed port for this policy.	option	-
	Option **Description** *enable* Enable fixed port for this policy. *disable* Disable fixed port for this policy.		
tcp-mss-sender	TCP Maximum Segment Size value of sender .	integer	Minimum value: 0 Maximum value: 65535
tcp-mss-receiver	TCP Maximum Segment Size value of receiver	integer	Minimum value: 0 Maximum value: 65535
comments	Comment.	var-string	Maximum length: 1023
ippool	Enable/disable use of IP Pools for source NAT.	option	-
	Option **Description** *enable* Enable use of IP Pools for source NAT. *disable* Disable use of IP Pools for source NAT.		
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79

config firewall proxy-policy

Configure proxy policies.

```
config firewall proxy-policy
   Description: Configure proxy policies.
   edit <policyid>
      set uuid {uuid}
      set proxy [explicit-web|transparent-web|...]
      set srcintf <name1>, <name2>, ...
      set dstintf <name1>, <name2>, ...
      set srcaddr <name1>, <name2>, ...
      set poolname <name1>, <name2>, ...
      set dstaddr <name1>, <name2>, ...
      set internet-service [enable|disable]
      set internet-service-negate [enable|disable]
      set internet-service-id <id1>, <id2>, ...
      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 ips-sensor {string}
      set application-list {string}
      set icap-profile {string}
      set cifs-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}
  next
end
```

config firewall proxy-policy

Parameter	Description	Type	Size
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
proxy	Type of explicit proxy.	option	-

Option	Description
explicit-web	Explicit Web Proxy
transparent-web	Transparent Web Proxy
ftp	Explicit FTP Proxy
ssh	SSH Proxy
ssh-tunnel	SSH Tunnel

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
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-

Option	Description
enable	Enable use of Internet Services in policy.
disable	Disable use of Internet Services in policy.

internet-service-negate	When enabled, Internet Services match against any internet service EXCEPT the selected Internet Service.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable negated Internet Service match. *disable* — Disable negated Internet Service match.		
internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
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 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	-
	Option / **Description** *enable* — Enable source address negate. *disable* — Disable destination address negate.		
dstaddr-negate	When enabled, destination addresses match against any address EXCEPT the specified destination addresses.	option	-
	Option / **Description** *enable* — Enable source address negate. *disable* — Disable destination address negate.		
service-negate	When enabled, services match against any service EXCEPT the specified destination services.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable negated service match. *disable* / Disable negated service match.		
action	Accept or deny traffic matching the policy parameters.	option	-
	Option / **Description** *accept* / Action accept. *deny* / Action deny. *redirect* / Action redirect.		
status	Enable/disable the active status of the policy.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
schedule	Name of schedule object.	string	Maximum length: 35
logtraffic	Enable/disable logging traffic through the policy.	option	-
	Option / **Description** *all* / Log all sessions. *utm* / UTM event and matched application traffic log. *disable* / Disable traffic and application log.		
session-ttl	TTL in seconds for sessions accepted by this policy .	integer	Minimum value: 300 Maximum value: 2764800
srcaddr6 <name>	IPv6 source address objects. Address name.	string	Maximum length: 79
dstaddr6 <name>	IPv6 destination address objects. Address name.	string	Maximum length: 79
groups <name>	Names of group objects. Group name.	string	Maximum length: 79
users <name>	Names of user objects. Group name.	string	Maximum length: 79

Parameter	Description	Type	Size
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-

Option	Description
enable	Enable SSH policy redirect.
disable	Disable SSH policy redirect.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable use of IP address of client to connect to server.
disable	Disable use of IP address of client to connect to server.

Parameter	Description	Type	Size
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-

Option	Description
disable	Disable disclaimer.
domain	Display disclaimer for domain
policy	Display disclaimer for policy
user	Display disclaimer for current user

Parameter	Description	Type	Size
utm-status	Enable the use of UTM profiles/sensors/lists.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-

Option	Description
single	Do not allow security profile groups.
group	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
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
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
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35
application-list	Name of an existing Application list.	string	Maximum length: 35
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35
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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / 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

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
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
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
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified

config firewall multicast-policy

Configure multicast NAT policies.

```
config firewall multicast-policy
   Description: Configure multicast NAT policies.
   edit <id>
      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
status	Enable/disable this policy.	option	-
	Option / **Description** *enable* — Enable this policy. *disable* — Disable this policy.		
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-
	Option / **Description** *enable* — Enable logging traffic accepted by this policy. *disable* — 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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable source NAT. *disable* — Disable source NAT.		
snat-ip	IPv4 address to be used as the source address for NATed traffic.	ipv4-address	Not Specified
dnat	IPv4 DNAT address used for multicast destination addresses.	ipv4-address-any	Not Specified
action	Accept or deny traffic matching the policy.	option	-
	Option / **Description** *accept* — Accept traffic matching the policy. *deny* — 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
start-port	Integer value for starting TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535
end-port	Integer value for ending TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-
	Option / **Description** *enable* — Enable hardware acceleration offloading. *disable* — 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 status [enable|disable]
      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]
   next
end
```

config firewall multicast-policy6

Parameter	Description	Type	Size
status	Enable/disable this policy.	option	-
	Option / **Description** *enable* / Enable this policy. *disable* / Disable this policy.		
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-
	Option / **Description** *enable* / Enable logging traffic accepted by this policy. *disable* / 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	-
	Option / **Description** *accept* / Accept. *deny* / Deny.		

Parameter	Description	Type	Size
protocol	Integer value for the protocol type as defined by IANA .	integer	Minimum value: 0 Maximum value: 255
start-port	Integer value for starting TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535
end-port	Integer value for ending TCP/UDP/SCTP destination port in range .	integer	Minimum value: 0 Maximum value: 65535
auto-asic-offload	Enable/disable offloading policy traffic for hardware acceleration.	option	-

Option	Description
enable	Enable offloading policy traffic for hardware acceleration.
disable	Disable offloading policy traffic for hardware acceleration.

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
status	Enable/disable this policy.	option	-
	Option / **Description** *enable* — Enable this policy. *disable* — 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	-
	Option / **Description** *all* — Log all sessions accepted or denied by this policy. *utm* — Log traffic that has a security profile applied to it. *disable* — Disable all logging for this policy.		
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	-
	Option / **Description** *enable* — Enable application control *disable* — Disable application control		
application-list	Application list name.	string	Maximum length: 35
ips-sensor-status	Enable/disable IPS.	option	-

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

Parameter	Description	Type	Size
dlp-sensor-status	Enable/disable DLP.	option	-

Option	Description
enable	Enable setting.
disable	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
status	Enable/disable this policy.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable this policy. *disable* / 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** / **Description** *all* / Log all sessions accepted or denied by this policy. *utm* / Log traffic that has a security profile applied to it. *disable* / Disable all logging for this policy.	option	-
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** / **Description** *enable* / Enable application control *disable* / Disable application control	option	-
application-list	Application list name.	string	Maximum length: 35
ips-sensor-status	Enable/disable IPS.	option	-

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

Parameter	Description	Type	Size
dlp-sensor-status	Enable/disable DLP.	option	-

Option	Description
enable	Enable setting.
disable	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 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
status	Enable/disable this policy.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable this policy. *disable* Disable this policy.		
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. Service 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
status	Enable/disable this anomaly.	option	-
	Option **Description** *disable* Disable this status. *enable* Enable this status.		
log	Enable/disable anomaly logging.	option	-
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		
action	Action taken when the threshold is reached.	option	-
	Option **Description** *pass* Allow traffic but record a log message if logging is enabled. *block* Block traffic if this anomaly is found.		
quarantine	Quarantine method.	option	-

Parameter	Description	Type	Size
	Option / **Description** *none* — Quarantine is disabled. *attacker* — Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-
	Option / **Description** *disable* — Disable quarantine logging. *enable* — Enable quarantine logging.		
threshold	Anomaly threshold. Number of detected instances per minute that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647
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

config firewall DoS-policy6

Configure IPv6 DoS policies.

```
config firewall DoS-policy6
   Description: Configure IPv6 DoS policies.
   edit <policyid>
      set status [enable|disable]
      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
status	Enable/disable this policy.	option	-
	Option / **Description** *enable* — Enable this policy. *disable* — Disable this policy.		
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. Service 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
status	Enable/disable this anomaly.	option	-
	Option / **Description** *disable* — Disable this status. *enable* — Enable this status.		
log	Enable/disable anomaly logging.	option	-
	Option / **Description** *enable* — Enable anomaly logging. *disable* — Disable anomaly logging.		

Parameter	Description	Type	Size
action	Action taken when the threshold is reached.	option	-

Option	Description
pass	Allow traffic but record a log message if logging is enabled.
block	Block traffic if this anomaly is found.

Parameter	Description	Type	Size
quarantine	Quarantine method.	option	-

Option	Description
none	Quarantine is disabled.
attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.

Parameter	Description	Type	Size
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-

Option	Description
disable	Disable quarantine logging.
enable	Enable quarantine logging.

Parameter	Description	Type	Size
threshold	Anomaly threshold. Number of detected instances per minute that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647
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

config firewall sniffer

Configure sniffer.

```
config firewall sniffer
   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 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
status	Enable/disable the active status of the sniffer.	option	-

Option	Description
enable	Enable sniffer status.
disable	Disable sniffer status.

Parameter	Description	Type	Size
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	option	-

Option	Description
all	Log all sessions accepted or denied by this policy.

Parameter	Description	Type	Size
	Option / **Description** *utm* — Log traffic that has a security profile applied to it. *disable* — Disable all logging for this policy.		
ipv6	Enable/disable sniffing IPv6 packets.	option	-
	Option / **Description** *enable* — Enable sniffer for IPv6 packets. *disable* — Disable sniffer for IPv6 packets.		
non-ip	Enable/disable sniffing non-IP packets.	option	-
	Option / **Description** *enable* — Enable sniffer for non-IP packets. *disable* — 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	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
application-list	Name of an existing application list.	string	Maximum length: 35
ips-sensor-status	Enable/disable IPS sensor.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35
dsri	Enable/disable DSRI.	option	-
	Option / **Description** *enable* / Enable DSRI. *disable* / Disable DSRI.		
av-profile-status	Enable/disable antivirus profile.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
av-profile	Name of an existing antivirus profile.	string	Maximum length: 35
webfilter-profile-status	Enable/disable web filter profile.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
webfilter-profile	Name of an existing web filter profile.	string	Maximum length: 35
emailfilter-profile-status	Enable/disable emailfilter.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35

Parameter	Description	Type	Size
dlp-sensor-status	Enable/disable DLP sensor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35
ips-dos-status	Enable/disable IPS DoS anomaly detection.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
max-packet-count	Maximum packet count .	integer	Minimum value: 1 Maximum value: 10000 **

** Values may differ between models.

config anomaly

Parameter	Description	Type	Size
status	Enable/disable this anomaly.	option	-

Option	Description
disable	Disable this status.
enable	Enable this status.

Parameter	Description	Type	Size
log	Enable/disable anomaly logging.	option	-

Option	Description
enable	Enable anomaly logging.
disable	Disable anomaly logging.

Parameter	Description	Type	Size
action	Action taken when the threshold is reached.	option	-

Parameter	Description	Type	Size
	Option / **Description** *pass* — Allow traffic but record a log message if logging is enabled. *block* — Block traffic if this anomaly is found.		
quarantine	Quarantine method.	option	-
	Option / **Description** *none* — Quarantine is disabled. *attacker* — Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-
	Option / **Description** *disable* — Disable quarantine logging. *enable* — Enable quarantine logging.		
threshold	Anomaly threshold. Number of detected instances per minute that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647
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

config firewall central-snat-map

Configure central SNAT policies.

```
config firewall central-snat-map
   Description: Configure central SNAT policies.
   edit <policyid>
      set status [enable|disable]
      set orig-addr <name1>, <name2>, ...
      set srcintf <name1>, <name2>, ...
      set dst-addr <name1>, <name2>, ...
      set dstintf <name1>, <name2>, ...
      set nat-ippool <name1>, <name2>, ...
      set protocol {integer}
      set orig-port {user}
```

```
    set nat-port {user}
    set nat [disable|enable]
    set comments {var-string}
  next
end
```

config firewall central-snat-map

Parameter	Description	Type	Size
status	Enable/disable the active status of this policy.	option	-
	Option / **Description** *enable* — Enable this policy. *disable* — Disable this policy.		
orig-addr <name>	Original address. Address name.	string	Maximum length: 79
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79
dst-addr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79
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
protocol	Integer value for the protocol type .	integer	Minimum value: 0 Maximum value: 255
orig-port	Original TCP port (0 to 65535).	user	Not Specified
nat-port	Translated port or port range (0 to 65535).	user	Not Specified
nat	Enable/disable source NAT.	option	-
	Option / **Description** *disable* — Disable source NAT. *enable* — Enable source NAT.		
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
proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process .	integer	Minimum value: 1 Maximum value: 60
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-

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.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Send empty fragments.
disable	Do not send empty fragments.

Parameter	Description	Type	Size
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-

Parameter	Description	Type	Size
	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
cert-cache-timeout	Time limit to keep certificate cache .	integer	Minimum value: 1 Maximum value: 120
session-cache-capacity	Capacity of the SSL session cache .	integer	Minimum value: 0 Maximum value: 1000
session-cache-timeout	Time limit to keep SSL session state .	integer	Minimum value: 1 Maximum value: 60
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
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
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-
	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 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
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	-

Option	Description
built-in	Built-in SSH proxy local keys.
user	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
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	-

Parameter	Description	Type	Size
	Option / **Description** *built-in* / Built-in SSH proxy local keys. *user* / 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
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
host-trusted-checking	Enable/disable host trusted checking.	option	-

Option	Description
enable	Enable host key trusted checking.
disable	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 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
status	Set the trust status of the public key.	option	-

Option	Description
trusted	The public key is trusted.
revoked	The public key is revoked.

Parameter	Description	Type	Size
type	Set the type of the public key.	option	-

Option	Description
RSA	The type of the public key is RSA.
DSA	The type of the public key is DSA.
ECDSA	The type of the public key is ECDSA.
ED25519	The type of the public key is ED25519.

Parameter	Description	Type	Size
	Option / **Description** *RSA-CA* — The type of the public key is from RSA CA. *DSA-CA* — The type of the public key is from DSA CA. *ECDSA-CA* — The type of the public key is from ECDSA CA. *ED25519-CA* — The type of the public key is from ED25519 CA.		
nid	Set the nid of the ECDSA key.	option	-
	Option / **Description** *256* — The NID is ecdsa-sha2-nistp256. *384* — The NID is ecdsa-sha2-nistp384. *521* — The NID is ecdsa-sha2-nistp521.		
ip	IP address of the SSH server.	ipv4-address-any	Not Specified
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295
hostname	Hostname of the SSH server.	string	Maximum length: 255
public-key	SSH public key.	var-string	Maximum length: 32768

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
type	IP translation type (option: SCTP).	option	-

Option	Description
SCTP	SCTP

startip	First IPv4 address .	ipv4-address-any	Not Specified
endip	Final IPv4 address .	ipv4-address-any	Not Specified
map-startip	Address to be used as the starting point for translation in the range .	ipv4-address-any	Not Specified

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
hop-opt	Enable/disable blocking packets with the Hop-by-Hop Options header .	option	-

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	Enable/disable blocking packets with Destination Options headers .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable blocking packets with Destination Options headers. *disable* / Disable blocking packets with Destination Options headers.		
hdopt-type	Block specific Hop-by-Hop and/or Destination Option types .	integer	Minimum value: 0 Maximum value: 255
routing	Enable/disable blocking packets with Routing headers .	option	-
	Option / **Description** *enable* / Block packets with Routing headers. *disable* / Allow packets with Routing headers.		
routing-type	Block specific Routing header types .	integer	Minimum value: 0 Maximum value: 255
fragment	Enable/disable blocking packets with the Fragment header .	option	-
	Option / **Description** *enable* / Block packets with the Fragment header. *disable* / Allow packets with the Fragment header.		
auth	Enable/disable blocking packets with the Authentication header .	option	-
	Option / **Description** *enable* / Block packets with the Authentication header. *disable* / Allow packets with the Authentication header.		
no-next	Enable/disable blocking packets with the No Next header	option	-
	Option / **Description** *enable* / Block packets with the No Next header. *disable* / 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
<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
<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 370

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
status	Enable/disable the explicit FTP proxy.	option	-
	Option / **Description** *enable* — Enable the explicit FTP proxy. *disable* — 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	-

Parameter	Description	Type	Size
	Option / **Description** *accept* — Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not *deny* — Deny requests unless there is a matching explicit FTP proxy policy.		
ssl	Enable/disable the explicit FTPS proxy.	option	-
	Option / **Description** *enable* — Enable the explicit FTPS proxy. *disable* — Disable the explicit FTPS proxy.		
ssl-cert	Name of certificate for SSL connections to this server .	string	Maximum length: 35
ssl-dh-bits	Bit-size of Diffie-Hellman .	option	-
	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	-
	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.		

hardware

This section includes syntax for the following commands:

- config hardware nic on page 372
- config hardware cpu on page 372
- config hardware status on page 372
- config hardware memory on page 372

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
<nic>	NIC name.	string	Maximum length: -1

icap

This section includes syntax for the following commands:

- config icap profile on page 375
- config icap server on page 374

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}
   next
end
```

config icap server

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

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]
      config icap-headers
         Description: Configure ICAP forwarded request headers.
         edit <id>
            set name {string}
            set content {string}
            set base64-encoding [disable|enable]
         next
      end
   next
end
```

config icap profile

Parameter	Description	Type	Size
replacemsg-group	Replacement message group.	string	Maximum length: 35
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-

Option	Description
disable	Disable HTTP request passing to ICAP server.
enable	Enable HTTP request passing to ICAP server.

Parameter	Description	Type	Size
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-

Option	Description
disable	Disable HTTP response passing to ICAP server.

Parameter	Description	Type	Size
	Option **Description** *enable* Enable HTTP response passing to ICAP server.		
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-
	Option **Description** *disable* Disable bypassing of ICAP server for streaming content. *enable* Enable bypassing of ICAP server for streaming content.		
preview	Enable/disable preview of data to ICAP server.	option	-
	Option **Description** *disable* Disable preview of data to ICAP server. *enable* 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
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	-
	Option **Description** *error* Error. *bypass* Bypass.		
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-
	Option **Description** *error* Error. *bypass* Bypass.		
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127

Parameter	Description	Type	Size
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	-

Option	Description
delete	Forward HTTP request or response with DELETE method to ICAP server for further processing.
get	Forward HTTP request or response with GET method to ICAP server for further processing.
head	Forward HTTP request or response with HEAD method to ICAP server for further processing.
options	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.
post	Forward HTTP request or response with POST method to ICAP server for further processing.
put	Forward HTTP request or response with PUT method to ICAP server for further processing.
trace	Forward HTTP request or response with TRACE method to ICAP server for further processing.
other	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	-

Option	Description
disable	Do not add req-hdr for response modification (respmod) processing.
enable	Add req-hdr for response modification (respmod) processing.

config icap-headers

Parameter	Description	Type	Size
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	-

Parameter	Description	Type	Size

Option	Description
disable	Disable use of base64 encoding of HTTP content.
enable	Enable use of base64 encoding of HTTP content.

ips

This section includes syntax for the following commands:

- config ips rule on page 388
- config ips custom on page 390
- config ips global on page 392
- config ips rule-settings on page 390
- config ips sensor on page 379
- config ips settings on page 396
- config ips view-map on page 387
- config ips session on page 397
- config ips decoder on page 388

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 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
   config filter
      Description: IPS sensor filter.
      edit <name>
         set location {user}
         set severity {user}
         set protocol {user}
         set os {user}
         set application {user}
         set status [disable|enable|...]
         set log [disable|enable]
         set log-packet [disable|enable]
         set action [pass|block|...]
         set quarantine [none|attacker]
         set quarantine-expiry {integer}
         set quarantine-log [disable|enable]
      next
   end
   config override
      Description: IPS override rule.
      edit <rule-id>
         set status [disable|enable]
         set log [disable|enable]
         set log-packet [disable|enable]
         set action [pass|block|...]
         set quarantine [none|attacker]
         set quarantine-expiry {integer}
         set quarantine-log [disable|enable]
         config exempt-ip
            Description: Exempted IP.
            edit <id>
               set src-ip {ipv4-classnet}
               set dst-ip {ipv4-classnet}
            next
         end
      next
   end
 next
end
```

config ips sensor

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

Parameter	Description	Type	Size
replacemsg-group	Replacement message group.	string	Maximum length: 35
block-malicious-url	Enable/disable malicious URL blocking.	option	-

Option	Description
disable	Disable malicious URL blocking.
enable	Enable malicious URL blocking.

scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-

Option	Description
disable	Do not scan connections to botnet servers.
block	Block connections to botnet servers.
monitor	Log connections to botnet servers.

extended-log	Enable/disable extended logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

config entries

Parameter	Description	Type	Size
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
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified
protocol	Protocols to be examined. set protocol ? lists available protocols. all includes all protocols. other includes all unlisted protocols.	user	Not Specified

Parameter	Description	Type	Size
os	Operating systems to be protected. all includes all operating systems. other includes all unlisted operating systems.	user	Not Specified
application	Applications to be protected. set application ? lists available applications. all includes all applications. other includes all unlisted applications.	user	Not Specified
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	-

Option	Description
disable	Disable status of selected rules.
enable	Enable status of selected rules.
default	Default.

log	Enable/disable logging of signatures included in filter.	option	-

Option	Description
disable	Disable logging of selected rules.
enable	Enable logging of selected rules.

log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-

Option	Description
disable	Disable packet logging of selected rules.
enable	Enable packet logging of selected rules.

log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-

Option	Description
disable	Disable logging of detailed attack context.
enable	Enable logging of detailed attack context.

action	Action taken with traffic in which signatures are detected.	option	-

Parameter	Description	Type	Size
	Option / **Description** *pass* — Pass or allow matching traffic. *block* — Block or drop matching traffic. *reset* — Reset sessions for matching traffic. *default* — 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
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535
rate-mode	Rate limit mode.	option	-
	Option / **Description** *periodical* — Allow configured number of packets every rate-duration. *continuous* — Block packets once the rate is reached.		
rate-track	Track the packet protocol field.	option	-
	Option / **Description** *none* — none *src-ip* — Source IP. *dest-ip* — Destination IP. *dhcp-client-mac* — DHCP client. *dns-domain* — DNS domain.		
quarantine	Quarantine method.	option	-
	Option / **Description** *none* — Quarantine is disabled. *attacker* — Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine. . Requires quarantine set to attacker.	user	Not Specified

Parameter	Description	Type	Size
quarantine-log	Enable/disable quarantine logging.	option	-

Option	Description
disable	Disable quarantine logging.
enable	Enable quarantine logging.

config exempt-ip

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

config filter

Parameter	Description	Type	Size
location	Vulnerability location filter.	user	Not Specified
severity	Vulnerability severity filter.	user	Not Specified
protocol	Vulnerable protocol filter.	user	Not Specified
os	Vulnerable OS filter.	user	Not Specified
application	Vulnerable application filter.	user	Not Specified
status	Selected rules status.	option	-

Option	Description
disable	Disable status of selected rules.
enable	Enable status of selected rules.
default	Default.

log	Enable/disable logging of selected rules.	option	-

Option	Description
disable	Disable logging of selected rules.
enable	Enable logging of selected rules.

log-packet	Enable/disable packet logging of selected rules.	option	-

Option	Description
disable	Disable packet logging of selected rules.

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable packet logging of selected rules.		
action	Action of selected rules.	option	-
	Option / **Description** *pass* / Pass or allow matching traffic. *block* / Block or drop matching traffic. *reset* / Reset sessions for matching traffic. *default* / Pass or drop matching traffic, depending on the default action of the signature.		
quarantine	Quarantine IP or interface.	option	-
	Option / **Description** *none* / Quarantine is disabled. *attacker* / Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine in minute.	integer	Minimum value: 1 Maximum value: 2147483647
quarantine-log	Enable/disable logging of selected quarantine.	option	-
	Option / **Description** *disable* / Disable logging of selected quarantine. *enable* / Enable logging of selected quarantine.		

config override

Parameter	Description	Type	Size
status	Enable/disable status of override rule.	option	-
	Option / **Description** *disable* / Disable status of override rule. *enable* / Enable status of override rule.		
log	Enable/disable logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable logging. *enable* Enable logging.		
log-packet	Enable/disable packet logging.	option	-
	Option **Description** *disable* Disable packet logging. *enable* Enable packet logging.		
action	Action of override rule.	option	-
	Option **Description** *pass* Pass or allow matching traffic. *block* Block or drop matching traffic. *reset* Reset sessions for matching traffic.		
quarantine	Quarantine IP or interface.	option	-
	Option **Description** *none* Quarantine is disabled. *attacker* Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine in minute.	integer	Minimum value: 1 Maximum value: 2147483647
quarantine-log	Enable/disable logging of selected quarantine.	option	-
	Option **Description** *disable* Disable logging of selected quarantine. *enable* Enable logging of selected quarantine.		

config exempt-ip

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

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|firewall6|...]
   next
end
```

config ips view-map

Parameter	Description	Type	Size
vdom-id	VDOM ID.	integer	Minimum value: 0 Maximum value: 4294967295
policy-id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295
id-policy-id	ID-based policy ID.	integer	Minimum value: 0 Maximum value: 4294967295
which	Policy.	option	-

Option	Description
firewall	Firewall policy.
firewall6	Firewall policy6.
interface	Interface policy.
interface6	Interface policy6.
sniffer	Sniffer policy.
sniffer6	Sniffer policy6.
explicit	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
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
status	Enable/disable status.	option	-
	Option / **Description** *disable* — Disable status. *enable* — Enable status.		
log	Enable/disable logging.	option	-
	Option / **Description** *disable* — Disable logging. *enable* — Enable logging.		
log-packet	Enable/disable packet logging.	option	-
	Option / **Description** *disable* — Disable packet logging. *enable* — Enable packet logging.		
action	Action.	option	-
	Option / **Description** *pass* — Pass or allow matching traffic. *block* — 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

Parameter	Description	Type	Size
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295

config metadata

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

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
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095
rule-id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified
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	-

Option	Description
disable	Disable status.
enable	Enable status.

log	Enable/disable logging.	option	-

Option	Description
disable	Disable logging.
enable	Enable logging.

log-packet	Enable/disable packet logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable packet logging. *enable* — Enable packet logging.		
action	Default action (pass or block) for this signature. **Option** / **Description** *pass* — Pass or allow matching traffic. *block* — Block or drop matching traffic.	option	-
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 intelligent-mode [enable|disable]
   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 skype-client-public-ipaddr {var-string}
   set deep-app-insp-timeout {integer}
   set deep-app-insp-db-limit {integer}
   set exclude-signatures [none|industrial]
   set packet-log-queue-depth {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
fail-open	Enable to allow traffic if the IPS process crashes. Default is disable and IPS traffic is blocked when the IPS process crashes.	option	-

Option	Description
enable	Enable IPS fail open.
disable	Disable IPS fail open.

Parameter	Description	Type	Size
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-

Option	Description
regular	IPS regular database package.
extended	IPS extended database package.

Parameter	Description	Type	Size
traffic-submit	Enable/disable submitting attack data found by this FortiGate to FortiGuard.	option	-

Option	Description
enable	Enable traffic submit.
disable	Disable traffic submit.

Parameter	Description	Type	Size
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-

Option	Description
periodical	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.
continuous	Block packets once an anomaly is detected. Overrides individual anomaly settings.

Parameter	Description	Type	Size
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-

Option	Description
accurate	Accurately count concurrent sessions, demands more resources.

Parameter	Description	Type	Size
	Option / **Description** *heuristic* / Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.		
intelligent-mode	Enable/disable IPS adaptive scanning (intelligent mode). Intelligent mode optimizes the scanning method for the type of traffic.	option	-
	Option / **Description** *enable* / Enable intelligent scan mode. *disable* / Disable intelligent scan mode.		
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 **
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
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-
	Option / **Description** *enable* / Enable use of kernel session TTL for IPS sessions. *disable* / Disable use of kernel session TTL for IPS sessions.		
np-accel-mode *	Acceleration mode for IPS processing by NPx processors.	option	-
	Option / **Description** *none* / NPx acceleration disabled. *basic* / NPx acceleration enabled.		
cp-accel-mode *	IPS Pattern matching acceleration/offloading to CPx processors.	option	-
	Option / **Description** *none* / CPx acceleration/offloading disabled. *basic* / Offload basic pattern matching to CPx processors.		

Parameter	Description	Type	Size
	Option / **Description** *advanced* / Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.		
skype-client-public-ipaddr	Public IP addresses of your network that receive Skype sessions. Helps identify Skype sessions. Separate IP addresses with commas.	var-string	Maximum length: 255
deep-app-insp-timeout	Timeout for Deep application inspection .	integer	Minimum value: 0 Maximum value: 2147483647
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database	integer	Minimum value: 0 Maximum value: 2147483647
exclude-signatures	Excluded signatures.	option	-
	Option / **Description** *none* / No signatures excluded. *industrial* / Exclude industrial signatures.		
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096

* This parameter may not exist in some models.

** Values may differ between models.

config tls-active-probe

Parameter	Description	Type	Size
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option / **Description** *auto* / Set outgoing interface automatically. *sdwan* / Set outgoing interface by SD-WAN or policy routing rules.		

Parameter	Description	Type	Size
	Option: *specify* — Description: 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
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
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
packet-log-post-attack	Number of packets to log after the IPS signature is detected .	integer	Minimum value: 0 Maximum value: 255
packet-log-memory	Maximum memory can be used by packet log .	integer	Minimum value: 64 Maximum value: 8192
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

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 398

config ipsec tunnel

IPsec tunnel.

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

log

This section includes syntax for the following commands:

- config log syslogd setting on page 410
- config log custom-field on page 410
- config log fortianalyzer-cloud filter on page 528
- config log disk filter on page 467
- config log syslogd2 override-setting on page 425
- config log syslogd2 setting on page 421
- config log syslogd3 setting on page 432
- config log syslogd2 override-filter on page 430
- config log syslogd4 override-setting on page 447
- config log gui-display on page 488
- config log syslogd4 filter on page 450
- config log fortianalyzer-cloud override-setting on page 528
- config log fortianalyzer2 setting on page 501
- config log fortiguard setting on page 475
- config log syslogd override-setting on page 414
- config log syslogd3 override-setting on page 436
- config log fortianalyzer2 filter on page 509
- config log fortiguard override-filter on page 480
- config log memory global-setting on page 456
- config log syslogd4 override-filter on page 452
- config log memory filter on page 458
- config log fortianalyzer-cloud setting on page 525
- config log fortianalyzer2 override-filter on page 511
- config log threat-weight on page 400
- config log fortianalyzer3 setting on page 513
- config log memory setting on page 457
- config log fortianalyzer3 override-filter on page 523
- config log fortianalyzer3 filter on page 521
- config log fortianalyzer filter on page 497
- config log fortianalyzer setting on page 489
- config log fortianalyzer3 override-setting on page 517
- config log syslogd2 filter on page 428
- config log fortiguard override-setting on page 477
- config log disk setting on page 463
- config log webtrends setting on page 454
- config log fortianalyzer2 override-setting on page 505
- config log syslogd3 override-filter on page 441
- config log syslogd3 filter on page 439
- config log null-device filter on page 483

- config log webtrends filter on page 455
- config log setting on page 484
- config log syslogd4 setting on page 443
- config log fortianalyzer override-filter on page 499
- config log fortiguard filter on page 478
- config log fortianalyzer-cloud override-filter on page 530
- config log eventfilter on page 472
- config log syslogd override-filter on page 419
- config log fortianalyzer override-setting on page 493
- config log syslogd filter on page 417
- config log null-device setting on page 482

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 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 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
status	Enable/disable the threat weight feature.	option	-

Option	Description
enable	Enable the threat weight feature.
disable	Disable the threat weight feature.

blocked-connection	Threat weight score for blocked connections.	option	-

Option	Description
disable	Disable threat weight scoring for blocked connections.
low	Use the low level score for blocked connections.
medium	Use the medium level score for blocked connections.
high	Use the high level score for blocked connections.
critical	Use the critical level score for blocked connections.

failed-connection	Threat weight score for failed connections.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable threat weight scoring for failed connections. *low* — Use the low level score for failed connections. *medium* — Use the medium level score for failed connections. *high* — Use the high level score for failed connections. *critical* — Use the critical level score for failed connections.		
url-block-detected	Threat weight score for URL blocking.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for URL blocking. *low* — Use the low level score for URL blocking. *medium* — Use the medium level score for URL blocking. *high* — Use the high level score for URL blocking. *critical* — Use the critical level score for URL blocking.		
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for detected botnet connections. *low* — Use the low level score for detected botnet connections. *medium* — Use the medium level score for detected botnet connections. *high* — Use the high level score for detected botnet connections. *critical* — Use the critical level score for detected botnet connections.		

config level

Parameter	Description	Type	Size
low	Low level score value .	integer	Minimum value: 1 Maximum value: 100

Parameter	Description	Type	Size
medium	Medium level score value .	integer	Minimum value: 1 Maximum value: 100
high	High level score value .	integer	Minimum value: 1 Maximum value: 100
critical	Critical level score value .	integer	Minimum value: 1 Maximum value: 100

config malware

Parameter	Description	Type	Size
virus-infected	Threat weight score for virus (infected) detected.	option	-

Option	Description
disable	Disable threat weight scoring for virus (infected) detected.
low	Use the low level score for virus (infected) detected.
medium	Use the medium level score for virus (infected) detected.
high	Use the high level score for virus (infected) detected.
critical	Use the critical level score for virus (infected) detected.

file-blocked	Threat weight score for blocked file detected.	option	-

Option	Description
disable	Disable threat weight scoring for blocked file detected.
low	Use the low level score for blocked file detected.
medium	Use the medium level score for blocked file detected.
high	Use the high level score for blocked file detected.
critical	Use the critical level score for blocked file detected.

command-blocked	Threat weight score for blocked command detected.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable threat weight scoring for blocked command detected. *low* — Use the low level score for blocked command detected. *medium* — Use the medium level score for blocked command detected. *high* — Use the high level score for blocked command detected. *critical* — Use the critical level score for blocked command detected.		
oversized	Threat weight score for oversized file detected.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for oversized file detected. *low* — Use the low level score for oversized file detected. *medium* — Use the medium level score for oversized file detected. *high* — Use the high level score for oversized file detected. *critical* — Use the critical level score for oversized file detected.		
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for virus (scan error) detected. *low* — Use the low level score for virus (scan error) detected. *medium* — Use the medium level score for virus (scan error) detected. *high* — Use the high level score for virus (scan error) detected. *critical* — Use the critical level score for virus (scan error) detected.		
switch-proto	Threat weight score for switch proto detected.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for switch proto detected. *low* — Use the low level score for switch proto detected. *medium* — Use the medium level score for switch proto detected. *high* — Use the high level score for switch proto detected. *critical* — Use the critical level score for switch proto detected.		
mimefragmented	Threat weight score for mimefragmented detected.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable threat weight scoring for mimefragmented detected. *low* — Use the low level score for mimefragmented detected. *medium* — Use the medium level score for mimefragmented detected. *high* — Use the high level score for mimefragmented detected. *critical* — Use the critical level score for mimefragmented detected.		
virus-file-type-executable	Threat weight score for virus (filetype executable) detected.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for virus (filetype executable) detected. *low* — Use the low level score for virus (filetype executable) detected. *medium* — Use the medium level score for virus (filetype executable) detected. *high* — Use the high level score for virus (filetype executable) detected. *critical* — Use the critical level score for virus (filetype executable) detected.		
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for virus (outbreak prevention) event. *low* — Use the low level score for virus (outbreak prevention) event. *medium* — Use the medium level score for virus (outbreak prevention) event. *high* — Use the high level score for virus (outbreak prevention) event. *critical* — Use the critical level score for virus (outbreak prevention) event.		
content-disarm	Threat weight score for virus (content disarm) detected.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for virus (content disarm) detected. *low* — Use the low level score for virus (content disarm) detected. *medium* — Use the medium level score for virus (content disarm) detected. *high* — Use the high level score for virus (content disarm) detected. *critical* — Use the critical level score for virus (content disarm) detected.		

Parameter	Description	Type	Size
malware-list	Threat weight score for virus (malware list) detected.	option	-

Option	Description
disable	Disable threat weight scoring for virus (malware list) detected.
low	Use the low level score for virus (malware list) detected.
medium	Use the medium level score for virus (malware list) detected.
high	Use the high level score for virus (malware list) detected.
critical	Use the critical level score for virus (malware list) detected.

fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-

Option	Description
disable	Disable threat weight scoring for FortiSandbox malicious malware detected.
low	Use the low level score for FortiSandbox malicious malware detected.
medium	Use the medium level score for FortiSandbox malicious malware detected.
high	Use the high level score for FortiSandbox malicious malware detected.
critical	Use the critical level score for FortiSandbox malicious malware detected.

fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-

Option	Description
disable	Disable threat weight scoring for FortiSandbox high risk malware detected.
low	Use the low level score for FortiSandbox high risk malware detected.
medium	Use the medium level score for FortiSandbox high risk malware detected.
high	Use the high level score for FortiSandbox high risk malware detected.
critical	Use the critical level score for FortiSandbox high risk malware detected.

fsa-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-

Parameter	Description	Type	Size

Option	Description
disable	Disable threat weight scoring for FortiSandbox medium risk malware detected.
low	Use the low level score for FortiSandbox medium risk malware detected.
medium	Use the medium level score for FortiSandbox medium risk malware detected.
high	Use the high level score for FortiSandbox medium risk malware detected.
critical	Use the critical level score for FortiSandbox medium risk malware detected.

config ips

Parameter	Description	Type	Size
info-severity	Threat weight score for IPS info severity events.	option	-

Option	Description
disable	Disable threat weight scoring for IPS info severity events.
low	Use the low level score for IPS info severity events.
medium	Use the medium level score for IPS info severity events.
high	Use the high level score for IPS info severity events.
critical	Use the critical level score for IPS info severity events.

low-severity	Threat weight score for IPS low severity events.	option	-

Option	Description
disable	Disable threat weight scoring for IPS low severity events.
low	Use the low level score for IPS low severity events.
medium	Use the medium level score for IPS low severity events.
high	Use the high level score for IPS low severity events.
critical	Use the critical level score for IPS low severity events.

medium-severity	Threat weight score for IPS medium severity events.	option	-

Option	Description
disable	Disable threat weight scoring for IPS medium severity events.

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

config web

Parameter	Description	Type	Size
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255
level	Threat weight score for web category filtering matches.	option	-
	Option / **Description** *disable* — Disable threat weight scoring for web category filtering matches. *low* — Use the low level score for web category filtering matches.		

Parameter	Description	Type	Size
	Option **Description** *medium* Use the medium level score for web category filtering matches. *high* Use the high level score for web category filtering matches. *critical* Use the critical level score for web category filtering matches.		

config geolocation

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

config application

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

config log 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
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 syslogd setting

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

Parameter	Description	Type	Size
server	Address of remote syslog server.	string	Maximum length: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

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
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).

Parameter	Description	Type	Size
	Option / **Description** *ftp* / FTP daemon. *ntp* / NTP daemon. *audit* / Log audit. *alert* / Log alert. *clock* / Clock daemon. *local0* / Reserved for local use. *local1* / Reserved for local use. *local2* / Reserved for local use. *local3* / Reserved for local use. *local4* / Reserved for local use. *local5* / Reserved for local use. *local6* / Reserved for local use. *local7* / Reserved for local use.		
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-
	Option / **Description** *default* / Syslog format. *csv* / CSV (Comma Separated Values) format. *cef* / CEF (Common Event Format) format.		
priority	Set log transmission priority.	option	-
	Option / **Description** *default* / Set Syslog transmission priority to default. *low* / Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size
	Option **Description** *high-medium* SSL communication with high and medium encryption algorithms. *high* SSL communication with high encryption algorithms. *low* SSL communication with low encryption algorithms. *disable* Disable SSL communication.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option **Description** *default* Follow system global setting. *SSLv3* SSLv3. *TLSv1* TLSv1. *TLSv1-1* TLSv1.1. *TLSv1-2* 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	-
	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 custom-field-name

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

Parameter	Description	Type	Size
server	Address of remote syslog server.	string	Maximum length: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

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
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

Parameter	Description	Type	Size
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-

Option	Description
default	Syslog format.
csv	CSV (Comma Separated Values) format.
cef	CEF (Common Event Format) format.

priority	Set log transmission priority.	option	-

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
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	-

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 custom-field-name

Parameter	Description	Type	Size
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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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
status	Enable/disable remote syslog logging.	option	-

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: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).

Parameter	Description	Type	Size
	Option / **Description** *ftp* — FTP daemon. *ntp* — NTP daemon. *audit* — Log audit. *alert* — Log alert. *clock* — Clock daemon. *local0* — Reserved for local use. *local1* — Reserved for local use. *local2* — Reserved for local use. *local3* — Reserved for local use. *local4* — Reserved for local use. *local5* — Reserved for local use. *local6* — Reserved for local use. *local7* — Reserved for local use.		
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format.		
priority	Set log transmission priority.	option	-
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size
	Option **Description** *high-medium* SSL communication with high and medium encryption algorithms. *high* SSL communication with high encryption algorithms. *low* SSL communication with low encryption algorithms. *disable* Disable SSL communication.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option **Description** *default* Follow system global setting. *SSLv3* SSLv3. *TLSv1* TLSv1. *TLSv1-1* TLSv1.1. *TLSv1-2* 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	-
	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 custom-field-name

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

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: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

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
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

Parameter	Description	Type	Size
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-

Option	Description
default	Syslog format.
csv	CSV (Comma Separated Values) format.
cef	CEF (Common Event Format) format.

priority	Set log transmission priority.	option	-

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
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	-

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 custom-field-name

Parameter	Description	Type	Size
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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd2 filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog 2 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd2 override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog 2 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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
status	Enable/disable remote syslog logging.	option	-

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: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).

Parameter	Description	Type	Size
	Option / **Description** *ftp* / FTP daemon. *ntp* / NTP daemon. *audit* / Log audit. *alert* / Log alert. *clock* / Clock daemon. *local0* / Reserved for local use. *local1* / Reserved for local use. *local2* / Reserved for local use. *local3* / Reserved for local use. *local4* / Reserved for local use. *local5* / Reserved for local use. *local6* / Reserved for local use. *local7* / Reserved for local use.		
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-
	Option / **Description** *default* / Syslog format. *csv* / CSV (Comma Separated Values) format. *cef* / CEF (Common Event Format) format.		
priority	Set log transmission priority.	option	-
	Option / **Description** *default* / Set Syslog transmission priority to default. *low* / Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size
	Option / **Description** *high-medium* — SSL communication with high and medium encryption algorithms. *high* — SSL communication with high encryption algorithms. *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — 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	-
	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 custom-field-name

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

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: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

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
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

Parameter	Description	Type	Size
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-

Option	Description
default	Syslog format.
csv	CSV (Comma Separated Values) format.
cef	CEF (Common Event Format) format.

priority	Set log transmission priority.	option	-

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
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	-

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 custom-field-name

Parameter	Description	Type	Size
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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd3 filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog 3 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd3 override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog 3 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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
status	Enable/disable remote syslog logging.	option	-

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: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

Option	Description
udp	Enable syslogging over UDP.
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).

Parameter	Description	Type	Size
	Option / **Description** *ftp* / FTP daemon. *ntp* / NTP daemon. *audit* / Log audit. *alert* / Log alert. *clock* / Clock daemon. *local0* / Reserved for local use. *local1* / Reserved for local use. *local2* / Reserved for local use. *local3* / Reserved for local use. *local4* / Reserved for local use. *local5* / Reserved for local use. *local6* / Reserved for local use. *local7* / Reserved for local use.		
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-
	Option / **Description** *default* / Syslog format. *csv* / CSV (Comma Separated Values) format. *cef* / CEF (Common Event Format) format.		
priority	Set log transmission priority.	option	-
	Option / **Description** *default* / Set Syslog transmission priority to default. *low* / Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size
	Option **Description** *high-medium* SSL communication with high and medium encryption algorithms. *high* SSL communication with high encryption algorithms. *low* SSL communication with low encryption algorithms. *disable* Disable SSL communication.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option **Description** *default* Follow system global setting. *SSLv3* SSLv3. *TLSv1* TLSv1. *TLSv1-1* TLSv1.1. *TLSv1-2* 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	-
	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 custom-field-name

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

Option	Description
enable	Log to remote syslog server.
disable	Do not log to remote syslog server.

Parameter	Description	Type	Size
server	Address of remote syslog server.	string	Maximum length: 63
mode	Remote syslog logging over UDP/Reliable TCP.	option	-

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
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
facility	Remote syslog facility.	option	-

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

Parameter	Description	Type	Size
source-ip	Source IP address of syslog.	string	Maximum length: 63
format	Log format.	option	-

Option	Description
default	Syslog format.
csv	CSV (Comma Separated Values) format.
cef	CEF (Common Event Format) format.

priority	Set log transmission priority.	option	-

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
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	-

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 custom-field-name

Parameter	Description	Type	Size
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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd4 filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog 4 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log syslogd4 override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	Syslog 4 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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
status	Enable/disable logging to WebTrends.	option	-
	Option / **Description** *enable* / Enable logging to WebTrends. *disable* / Disble 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log webtrends filter

Parameter	Description	Type	Size
severity	Lowest severity level to log to WebTrends.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

Parameter	Description	Type	Size
multicast-traffic	Enable/disable multicast traffic logging.	option	-

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

Parameter	Description	Type	Size
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-

Option	Description
enable	Enable anomaly logging.
disable	Disable anomaly logging.

Parameter	Description	Type	Size
voip	Enable/disable VoIP logging.	option	-

Option	Description
enable	Enable VoIP logging.
disable	Disable VoIP logging.

Parameter	Description	Type	Size
filter	Webtrends log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log memory global-setting

Global settings for memory logging.

```
config log memory global-setting
   Description: Global settings for memory logging.
   set max-size {integer}
   set full-first-warning-threshold {integer}
   set full-second-warning-threshold {integer}
   set full-final-warning-threshold {integer}
```

```
end
```

config log memory global-setting

Parameter	Description	Type	Size
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295
full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100

config log memory setting

Settings for memory buffer.

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

config log memory setting

Parameter	Description	Type	Size
status	Enable/disable logging to the FortiGate's memory.	option	-

Option	Description
enable	Enable logging to memory.
disable	Disable logging to memory.

Parameter	Description	Type	Size
diskfull	Action to take when memory is full.	option	-

Parameter	Description	Type	Size

Option	Description
overwrite	Overwrite the oldest logs when the system memory reserved for logging is full.

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]
   set event [enable|disable]
   set system [enable|disable]
   set radius [enable|disable]
   set ipsec [enable|disable]
   set dhcp [enable|disable]
   set ppp [enable|disable]
   set admin [enable|disable]
   set ha [enable|disable]
   set auth [enable|disable]
   set pattern [enable|disable]
   set sslvpn-log-auth [enable|disable]
   set sslvpn-log-adm [enable|disable]
   set sslvpn-log-session [enable|disable]
   set vip-ssl [enable|disable]
   set ldb-monitor [enable|disable]
   set wan-opt [enable|disable]
   set wireless-activity [enable|disable]
   set cpu-memory-usage [enable|disable]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log memory filter

Parameter	Description	Type	Size
severity	Log every message above and including this severity level.	option	-

Parameter	Description	Type	Size
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.		
event	Enable/disable event logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
system	Enable/disable system activity logging.	option	-
	Option **Description** *enable* Enable system activity logging. *disable* Disable system activity logging.		
radius	Enable/disable RADIUS messages logging.	option	-
	Option **Description** *enable* Enable RADIUS messages logging. *disable* Disable RADIUS messages logging.		
ipsec	Enable/disable IPsec negotiation messages logging.	option	-
	Option **Description** *enable* Enable IPsec negotiation messages logging. *disable* Disable IPsec negotiation messages logging.		
dhcp	Enable/disable DHCP service messages logging.	option	-
	Option **Description** *enable* Enable DHCP service messages logging. *disable* Disable DHCP service messages logging.		
ppp	Enable/disable L2TP/PPTP/PPPoE logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable L2TP/PPTP/PPPoE logging. *disable* Disable L2TP/PPTP/PPPoE logging.		
admin	Enable/disable admin login/logout logging.	option	-
	Option **Description** *enable* Enable admin login/logout logging. *disable* Disable admin login/logout logging.		
ha	Enable/disable HA logging.	option	-
	Option **Description** *enable* Enable HA logging. *disable* Disable HA logging.		
auth	Enable/disable firewall authentication logging.	option	-
	Option **Description** *enable* Enable firewall authentication logging. *disable* Disable firewall authentication logging.		
pattern	Enable/disable pattern update logging.	option	-
	Option **Description** *enable* Enable pattern update logging. *disable* Disable pattern update logging.		
sslvpn-log-auth	Enable/disable SSL user authentication logging.	option	-
	Option **Description** *enable* Enable SSL user authentication logging. *disable* Disable SSL user authentication logging.		
sslvpn-log-adm	Enable/disable SSL administrator login logging.	option	-
	Option **Description** *enable* Enable SSL administrator logging. *disable* Disable SSL administrator logging.		

Parameter	Description	Type	Size
sslvpn-log-session	Enable/disable SSL session logging.	option	-

Option	Description
enable	Enable SSL session logging.
disable	Disable SSL session logging.

Parameter	Description	Type	Size
vip-ssl	Enable/disable VIP SSL logging.	option	-

Option	Description
enable	Enable VIP SSL logging.
disable	Disable VIP SSL logging.

Parameter	Description	Type	Size
ldb-monitor	Enable/disable VIP real server health monitoring logging.	option	-

Option	Description
enable	Enable VIP real server health monitoring logging.
disable	Disable VIP real server health monitoring logging.

Parameter	Description	Type	Size
wan-opt	Enable/disable WAN optimization event logging.	option	-

Option	Description
enable	Enable WAN optimization event logging.
disable	Disable WAN optimization event logging.

Parameter	Description	Type	Size
wireless-activity	Enable/disable wireless activity event logging.	option	-

Option	Description
enable	Enable wireless activity event logging.
disable	Disable wireless activity event logging.

Parameter	Description	Type	Size
cpu-memory-usage	Enable/disable CPU & memory usage logging every 5 minutes.	option	-

Option	Description
enable	Enable CPU & memory usage logging every 5 minutes.
disable	Disable CPU & memory usage logging every 5 minutes.

Parameter	Description	Type	Size
filter	Memory log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Option	Description
include	Include logs that match the filter.
exclude	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 uploaddir {string}
   set uploadtype {option1}, {option2}, ...
   set uploadsched [disable|enable]
   set uploadtime {user}
   set upload-delete-files [enable|disable]
   set upload-ssl-conn [default|high|...]
   set full-first-warning-threshold {integer}
   set full-second-warning-threshold {integer}
   set full-final-warning-threshold {integer}
end
```

config log disk setting

Parameter	Description	Type	Size
status	Enable/disable local disk logging.	option	-

Option	Description
enable	Log to local disk.
disable	Do not log to local disk.

Parameter	Description	Type	Size
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-

Option	Description
enable	Enable IPS packet archiving.
disable	Disable IPS packet archiving.

Parameter	Description	Type	Size
max-log-file-size	Maximum log file size before rolling .	integer	Minimum value: 1 Maximum value: 100
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295
roll-schedule	Frequency to check log file for rolling.	option	-

Option	Description
daily	Check the log file once a day.
weekly	Check the log file once a week.

Parameter	Description	Type	Size
roll-day	Day of week on which to roll log file.	option	-

Option	Description
sunday	Sunday
monday	Monday
tuesday	Tuesday
wednesday	Wednesday
thursday	Thursday
friday	Friday
saturday	Saturday

Parameter	Description	Type	Size
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	-

Option	Description
overwrite	Overwrite the oldest logs when the log disk is full.
nolog	Stop logging when the log disk is full.

log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650
upload	Enable/disable uploading log files when they are rolled.	option	-

Option	Description
enable	Enable uploading log files when they are rolled.
disable	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	-

Option	Description
ftp-server	Upload rolled log files to an FTP server.

uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified
uploadport	TCP port to use for communicating with the FTP server .	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified
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
uploaddir	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	-

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

uploadsched	Set the schedule for uploading log files to the FTP server .	option	-

Option	Description
disable	Upload when rolling.
enable	Scheduled upload.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Delete log files after uploading.
disable	Do not delete log files after uploading.

upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-

Option	Description
default	FTPS with high and medium encryption algorithms.
high	FTPS with high encryption algorithms.
low	FTPS with low encryption algorithms.
disable	Disable FTPS communication.

full-first-warning-threshold	Log full first warning threshold as a percent .	integer	Minimum value: 1 Maximum value: 98
full-second-warning-threshold	Log full second warning threshold as a percent .	integer	Minimum value: 2 Maximum value: 99
full-final-warning-threshold	Log full final warning threshold as a percent .	integer	Minimum value: 3 Maximum value: 100

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]
    set event [enable|disable]
    set system [enable|disable]
    set radius [enable|disable]
    set ipsec [enable|disable]
    set dhcp [enable|disable]
    set ppp [enable|disable]
    set admin [enable|disable]
    set ha [enable|disable]
    set auth [enable|disable]
    set pattern [enable|disable]
    set sslvpn-log-auth [enable|disable]
    set sslvpn-log-adm [enable|disable]
    set sslvpn-log-session [enable|disable]
    set vip-ssl [enable|disable]
    set ldb-monitor [enable|disable]
    set wan-opt [enable|disable]
    set wireless-activity [enable|disable]
    set cpu-memory-usage [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
end
```

config log disk filter

Parameter	Description	Type	Size
severity	Log to disk every message above and including this severity level.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

Parameter	Description	Type	Size
multicast-traffic	Enable/disable multicast traffic logging.	option	-

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

Parameter	Description	Type	Size
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-

Option	Description
enable	Enable anomaly logging.
disable	Disable anomaly logging.

Parameter	Description	Type	Size
voip	Enable/disable VoIP logging.	option	-

Option	Description
enable	Enable VoIP logging.
disable	Disable VoIP logging.

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

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
system	Enable/disable system activity logging.	option	-

Option	Description
enable	Enable system activity logging.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable system activity logging.		
radius	Enable/disable RADIUS messages logging.	option	-
	Option **Description** *enable* Enable RADIUS messages logging. *disable* Disable RADIUS messages logging.		
ipsec	Enable/disable IPsec negotiation messages logging.	option	-
	Option **Description** *enable* Enable IPsec negotiation messages logging. *disable* Disable IPsec negotiation messages logging.		
dhcp	Enable/disable DHCP service messages logging.	option	-
	Option **Description** *enable* Enable DHCP service messages logging. *disable* Disable DHCP service messages logging.		
ppp	Enable/disable L2TP/PPTP/PPPoE logging.	option	-
	Option **Description** *enable* Enable L2TP/PPTP/PPPoE logging. *disable* Disable L2TP/PPTP/PPPoE logging.		
admin	Enable/disable admin login/logout logging.	option	-
	Option **Description** *enable* Enable admin login/logout logging. *disable* Disable admin login/logout logging.		
ha	Enable/disable HA logging.	option	-
	Option **Description** *enable* Enable HA logging. *disable* Disable HA logging.		
auth	Enable/disable firewall authentication logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable firewall authentication logging. *disable* Disable firewall authentication logging.		
pattern	Enable/disable pattern update logging.	option	-
	Option **Description** *enable* Enable pattern update logging. *disable* Disable pattern update logging.		
sslvpn-log-auth	Enable/disable SSL user authentication logging.	option	-
	Option **Description** *enable* Enable SSL user authentication logging. *disable* Disable SSL user authentication logging.		
sslvpn-log-adm	Enable/disable SSL administrator login logging.	option	-
	Option **Description** *enable* Enable SSL administrator logging. *disable* Disable SSL administrator logging.		
sslvpn-log-session	Enable/disable SSL session logging.	option	-
	Option **Description** *enable* Enable SSL session logging. *disable* Disable SSL session logging.		
vip-ssl	Enable/disable VIP SSL logging.	option	-
	Option **Description** *enable* Enable VIP SSL logging. *disable* Disable VIP SSL logging.		
ldb-monitor	Enable/disable VIP real server health monitoring logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable VIP real server health monitoring logging. *disable* Disable VIP real server health monitoring logging.		
wan-opt	Enable/disable WAN optimization event logging.	option	-
	Option **Description** *enable* Enable WAN optimization event logging. *disable* Disable WAN optimization event logging.		
wireless-activity	Enable/disable wireless activity event logging.	option	-
	Option **Description** *enable* Enable wireless activity event logging. *disable* Disable wireless activity event logging.		
cpu-memory-usage	Enable/disable CPU & memory usage logging every 5 minutes.	option	-
	Option **Description** *enable* Enable CPU & memory usage logging every 5 minutes. *disable* Disable CPU & memory usage logging every 5 minutes.		
filter	Disk log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option **Description** *include* Include logs that match the filter. *exclude* 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]
end
```

config log eventfilter

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

Option	Description
enable	Enable event logging.
disable	Disable event logging.

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

Option	Description
enable	Enable system event logging.
disable	Disable system event logging.

Parameter	Description	Type	Size
vpn	Enable/disable VPN event logging.	option	-

Option	Description
enable	Enable VPN event logging.
disable	Disable VPN event logging.

Parameter	Description	Type	Size
user	Enable/disable user authentication event logging.	option	-

Option	Description
enable	Enable user authentication event logging.
disable	Disable user authentication event logging.

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

Option	Description
enable	Enable router event logging.
disable	Disable router event logging.

Parameter	Description	Type	Size
wireless-activity	Enable/disable wireless event logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable wireless event logging. *disable* Disable wireless event logging.		
wan-opt	Enable/disable WAN optimization event logging.	option	-
	Option **Description** *enable* Enable WAN optimization event logging. *disable* Disable WAN optimization event logging.		
endpoint	Enable/disable endpoint event logging.	option	-
	Option **Description** *enable* Enable endpoint event logging. *disable* Disable endpoint event logging.		
ha	Enable/disable ha event logging.	option	-
	Option **Description** *enable* Enable ha event logging. *disable* Disable ha event logging.		
security-rating	Enable/disable Security Rating result logging.	option	-
	Option **Description** *enable* Enable Security Fabric audit result logging. *disable* Disable Security Fabric audit result logging.		
fortiextender	Enable/disable FortiExtender logging.	option	-
	Option **Description** *enable* Enable Forti-Extender logging. *disable* Disable Forti-Extender logging.		
connector	Enable/disable SDN connector logging.	option	-
	Option **Description** *enable* Enable SDN connector logging. *disable* Disable SDN connector 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
status	Enable/disable logging to FortiCloud.	option	-

Option	Description
enable	Enable logging to FortiCloud.
disable	Disable logging to FortiCloud.

Parameter	Description	Type	Size
upload-option	Configure how log messages are sent to FortiCloud.	option	-

Option	Description
store-and-upload	Log to the hard disk and then upload logs to FortiCloud.
realtime	Log directly to FortiCloud in real time.
1-minute	Log directly to FortiCloud at 1-minute intervals.
5-minute	Log directly to FortiCloud at 5-minute intervals.

Parameter	Description	Type	Size
upload-interval	Frequency of uploading log files to FortiCloud.	option	-

Option	Description
daily	Upload log files to FortiCloud once a day.
weekly	Upload log files to FortiCloud once a week.
monthly	Upload log files to FortiCloud once a month.

Parameter	Description	Type	Size
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	-

Option	Description
default	Set FortiCloud log transmission priority to default.
low	Set FortiCloud log transmission priority to low.

Parameter	Description	Type	Size
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-

Option	Description
high-medium	Encrypt logs using high and medium encryption.
high	Encrypt logs using high encryption.
low	Encrypt logs using low encryption.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
conn-timeout	FortiGate Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Parameter	Description	Type	Size
	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 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
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-
	Option / **Description** *enable* — Override FortiCloud logging settings. *disable* — Use global FortiCloud logging settings.		
status	Enable/disable logging to FortiCloud.	option	-
	Option / **Description** *enable* — Enable logging to FortiCloud. *disable* — Disable logging to FortiCloud.		
upload-option	Configure how log messages are sent to FortiCloud.	option	-

Parameter	Description	Type	Size
	Option / **Description** *store-and-upload* — Log to the hard disk and then upload logs to FortiCloud. *realtime* — Log directly to FortiCloud in real time. *1-minute* — Log directly to FortiCloud at 1-minute intervals. *5-minute* — Log directly to FortiCloud at 5-minute intervals.		
upload-interval	Frequency of uploading log files to FortiCloud.	option	-
	Option / **Description** *daily* — Upload log files to FortiCloud once a day. *weekly* — Upload log files to FortiCloud once a week. *monthly* — Upload log files to FortiCloud once a month.		
upload-day	Day of week to roll logs.	user	Not Specified
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified
priority	Set log transmission priority.	option	-
	Option / **Description** *default* — Set FortiCloud log transmission priority to default. *low* — Set FortiCloud log transmission priority to low.		
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000

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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortiguard filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

Parameter	Description	Type	Size
multicast-traffic	Enable/disable multicast traffic logging.	option	-

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

Parameter	Description	Type	Size
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-

Option	Description
enable	Enable anomaly logging.
disable	Disable anomaly logging.

Parameter	Description	Type	Size
voip	Enable/disable VoIP logging.	option	-

Option	Description
enable	Enable VoIP logging.
disable	Disable VoIP logging.

Parameter	Description	Type	Size
filter	FortiCloud log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Option	Description
include	Include logs that match the filter.
exclude	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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortiguard override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* — Enable sniffer traffic logging. *disable* — Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
filter	FortiCloud log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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
status	Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	option	-
	Option / **Description** *enable* / Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved). *disable* / 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log null-device filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

Parameter	Description	Type	Size
multicast-traffic	Enable/disable multicast traffic logging.	option	-

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

Parameter	Description	Type	Size
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-

Option	Description
enable	Enable anomaly logging.
disable	Disable anomaly logging.

Parameter	Description	Type	Size
voip	Enable/disable VoIP logging.	option	-

Option	Description
enable	Enable VoIP logging.
disable	Disable VoIP logging.

Parameter	Description	Type	Size
filter	Null-device log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Option	Description
include	Include logs that match the filter.
exclude	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 log-policy-name [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
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-

Option	Description
enable	Enable adding resolved domain names to traffic logs.
disable	Disable adding resolved domain names to traffic logs.

Parameter	Description	Type	Size
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-

Option	Description
enable	Enable adding resolved service names to traffic logs.
disable	Disable adding resolved service names to traffic logs.

Parameter	Description	Type	Size
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-

Option	Description
enable	Enable logs with user-in-upper.
disable	Disable logs with user-in-upper.

Parameter	Description	Type	Size
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable implicit firewall policy logging. *disable* Disable implicit firewall policy logging.		
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-
	Option **Description** *enable* Enable implicit firewall policy6 logging. *disable* Disable implicit firewall policy6 logging.		
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-
	Option **Description** *enable* Enable invalid packet traffic logging. *disable* Disable invalid packet traffic logging.		
local-in-allow	Enable/disable local-in-allow logging.	option	-
	Option **Description** *enable* Enable local-in-allow logging. *disable* Disable local-in-allow logging.		
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-
	Option **Description** *enable* Enable local-in-deny-unicast logging. *disable* Disable local-in-deny-unicast logging.		
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-
	Option **Description** *enable* Enable local-in-deny-broadcast logging. *disable* Disable local-in-deny-broadcast logging.		
local-out	Enable/disable local-out logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable local-out logging. *disable* Disable local-out logging.		
daemon-log	Enable/disable daemon logging.	option	-
	Option **Description** *enable* Enable daemon logging. *disable* Disable daemon logging.		
neighbor-event	Enable/disable neighbor event logging.	option	-
	Option **Description** *enable* Enable neighbor event logging. *disable* Disable neighbor event logging.		
brief-traffic-format	Enable/disable brief format traffic logging.	option	-
	Option **Description** *enable* Enable brief format traffic logging. *disable* Disable brief format traffic logging.		
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-
	Option **Description** *enable* Enable anonymizing user names in log messages. *disable* Disable anonymizing user names in log messages.		
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-
	Option **Description** *enable* Enable explicit proxy firewall implicit policy logging. *disable* Disable explicit proxy firewall implicit policy logging.		
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable inserting policy comments into traffic logs. *disable* — Disable inserting policy comments into traffic logs.		
log-policy-name	Enable/disable inserting policy name into traffic logs.	option	-
	Option / **Description** *enable* — Enable inserting policy name into traffic logs. *disable* — Disable inserting policy name into traffic logs.		
faz-override	Enable/disable override FortiAnalyzer settings.	option	-
	Option / **Description** *enable* — Enable override FortiAnalyzer settings. *disable* — Disable override FortiAnalyzer settings.		
syslog-override	Enable/disable override Syslog settings.	option	-
	Option / **Description** *enable* — Enable override Syslog settings. *disable* — 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
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup	option	-

Option	Description
enable	Enable resolving IP addresses to hostnames.
disable	Disable resolving IP addresses to hostnames.

Parameter	Description	Type	Size
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-

Option	Description
enable	Enable unknown applications on the GUI.
disable	Disable unknown applications on the GUI.

Parameter	Description	Type	Size
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-

Option	Description
enable	Enable showing unscanned traffic.
disable	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 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
status	Enable/disable logging to FortiAnalyzer.	option	-
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 63
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-

Parameter	Description	Type	Size
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
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
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-

Option	Description
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.
realtime	Log directly to FortiAnalyzer in real time.
1-minute	Log directly to FortiAnalyzer at most every 1 minute.
5-minute	Log directly to FortiAnalyzer at most every 5 minutes.

upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-

Option	Description
daily	Upload log files to FortiAnalyzer once a day.
weekly	Upload log files to FortiAnalyzer once a week.
monthly	Upload log files to FortiAnalyzer once a month.

upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-

Option	Description
enable	Enable reliable logging to FortiAnalyzer.
disable	Disable reliable logging to FortiAnalyzer.

priority	Set log transmission priority.	option	-

Option	Description
default	Set FortiAnalyzer log transmission priority to default.
low	Set FortiAnalyzer log transmission priority to low.

max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

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

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer. *disable* — Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
status	Enable/disable logging to FortiAnalyzer.	option	-
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 63
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-

Parameter	Description	Type	Size
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
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
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-

Option	Description
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.
realtime	Log directly to FortiAnalyzer in real time.
1-minute	Log directly to FortiAnalyzer at most every 1 minute.
5-minute	Log directly to FortiAnalyzer at most every 5 minutes.

upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-

Option	Description
daily	Upload log files to FortiAnalyzer once a day.
weekly	Upload log files to FortiAnalyzer once a week.
monthly	Upload log files to FortiAnalyzer once a month.

upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-

Option	Description
enable	Enable reliable logging to FortiAnalyzer.
disable	Disable reliable logging to FortiAnalyzer.

priority	Set log transmission priority.	option	-

Option	Description
default	Set FortiAnalyzer log transmission priority to default.
low	Set FortiAnalyzer log transmission priority to low.

max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Parameter	Description	Type	Size
	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 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

Parameter	Description	Type	Size
multicast-traffic	Enable/disable multicast traffic logging.	option	-

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

Parameter	Description	Type	Size
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

Option	Description
enable	Enable sniffer traffic logging.
disable	Disable sniffer traffic logging.

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-

Option	Description
enable	Enable anomaly logging.
disable	Disable anomaly logging.

Parameter	Description	Type	Size
voip	Enable/disable VoIP logging.	option	-

Option	Description
enable	Enable VoIP logging.
disable	Disable VoIP logging.

Parameter	Description	Type	Size
dlp-archive	Enable/disable DLP archive logging.	option	-

Option	Description
enable	Enable DLP archive logging.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable DLP archive logging.		
filter	FortiAnalyzer log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter. **Option** **Description** *include* Include logs that match the filter. *exclude* Exclude logs that match the filter.	option	-

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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log. **Option** **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level.	option	-

Parameter	Description	Type	Size
	Option **Description** *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option **Description** *enable* Enable VoIP logging.		

Parameter	Description	Type	Size
	Option **Description** *disable* Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.		
filter	FortiAnalyzer log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option **Description** *include* Include logs that match the filter. *exclude* 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 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
status	Enable/disable logging to FortiAnalyzer.	option	-

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	Disable logging to FortiAnalyzer.

Parameter	Description	Type	Size
ips-archive	Enable/disable IPS packet archive logging.	option	-

Option	Description
enable	Enable IPS packet archive logging.
disable	Disable IPS packet archive logging.

Parameter	Description	Type	Size
server	The remote FortiAnalyzer.	string	Maximum length: 63
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-

Option	Description
enable	Enable identity verification of FortiAnalyzer by use of certificate.
disable	Disable identity verification of FortiAnalyzer by use of certificate.

Parameter	Description	Type	Size
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-

Option	Description
enable	Enable FortiAnalyzer access to configuration and data.
disable	Disable FortiAnalyzer access to configuration and data.

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

Option	Description
sha256	Use SHA256 as HMAC algorithm.
sha1	Step down to SHA1 as the HMAC algorithm.

Parameter	Description	Type	Size
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
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	-
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer. *realtime* — Log directly to FortiAnalyzer in real time. *1-minute* — Log directly to FortiAnalyzer at most every 1 minute.		

Parameter	Description	Type	Size
	Option **Description** *5-minute* Log directly to FortiAnalyzer at most every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option **Description** *daily* Upload log files to FortiAnalyzer once a day. *weekly* Upload log files to FortiAnalyzer once a week. *monthly* Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option **Description** *enable* Enable reliable logging to FortiAnalyzer. *disable* Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-
	Option **Description** *default* Set FortiAnalyzer log transmission priority to default. *low* Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	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 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 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
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-

Option	Description
enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.

status	Enable/disable logging to FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 63
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms.		

Parameter	Description	Type	Size
	Option / **Description** *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
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	-
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer. *realtime* — Log directly to FortiAnalyzer in real time.		

Parameter	Description	Type	Size
	Option / **Description** *1-minute* / Log directly to FortiAnalyzer at most every 1 minute. *5-minute* / Log directly to FortiAnalyzer at most every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option / **Description** *daily* / Upload log files to FortiAnalyzer once a day. *weekly* / Upload log files to FortiAnalyzer once a week. *monthly* / Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option / **Description** *enable* / Enable reliable logging to FortiAnalyzer. *disable* / Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-
	Option / **Description** *default* / Set FortiAnalyzer log transmission priority to default. *low* / Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	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 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer2 filter

Parameter	Description	Type	Size
severity	Log every message above and including this severity level.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.		
filter	FortiAnalyzer 2 log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Parameter	Description	Type	Size

Option	Description
include	Include logs that match the filter.
exclude	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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer2 override-filter

Parameter	Description	Type	Size
severity	Log every message above and including this severity level.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

forward-traffic	Enable/disable forward traffic logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.		

Parameter	Description	Type	Size
filter	FortiAnalyzer 2 log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Option	Description
include	Include logs that match the filter.
exclude	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 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
status	Enable/disable logging to FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable logging to FortiAnalyzer. *disable* Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option **Description** *enable* Enable IPS packet archive logging. *disable* Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 63
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option **Description** *enable* Enable identity verification of FortiAnalyzer by use of certificate. *disable* Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-
	Option **Description** *enable* Enable FortiAnalyzer access to configuration and data. *disable* Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option **Description** *sha256* Use SHA256 as HMAC algorithm. *sha1* Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms. *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
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	-
	Option / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer. *realtime* — Log directly to FortiAnalyzer in real time. *1-minute* — Log directly to FortiAnalyzer at most every 1 minute.		

Parameter	Description	Type	Size
	Option **Description** *5-minute* Log directly to FortiAnalyzer at most every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option **Description** *daily* Upload log files to FortiAnalyzer once a day. *weekly* Upload log files to FortiAnalyzer once a week. *monthly* Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option **Description** *enable* Enable reliable logging to FortiAnalyzer. *disable* Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-
	Option **Description** *default* Set FortiAnalyzer log transmission priority to default. *low* Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	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 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 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
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-

Option	Description
enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.

status	Enable/disable logging to FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable logging to FortiAnalyzer. *disable* — Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option / **Description** *enable* — Enable IPS packet archive logging. *disable* — Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 63
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option / **Description** *enable* — Enable identity verification of FortiAnalyzer by use of certificate. *disable* — Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-
	Option / **Description** *enable* — Enable FortiAnalyzer access to configuration and data. *disable* — Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option / **Description** *sha256* — Use SHA256 as HMAC algorithm. *sha1* — Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option / **Description** *high-medium* — Encrypt logs using high and medium encryption algorithms.		

Parameter	Description	Type	Size
	Option / **Description** *high* — Encrypt logs using high encryption algorithms. *low* — Encrypt logs using all encryption algorithms.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections . **Option** / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.	option	-
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
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** / **Description** *store-and-upload* — Log to hard disk and then upload to FortiAnalyzer. *realtime* — Log directly to FortiAnalyzer in real time.	option	-

Parameter	Description	Type	Size
	Option / **Description** *1-minute* / Log directly to FortiAnalyzer at most every 1 minute. *5-minute* / Log directly to FortiAnalyzer at most every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option / **Description** *daily* / Upload log files to FortiAnalyzer once a day. *weekly* / Upload log files to FortiAnalyzer once a week. *monthly* / Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option / **Description** *enable* / Enable reliable logging to FortiAnalyzer. *disable* / Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-
	Option / **Description** *default* / Set FortiAnalyzer log transmission priority to default. *low* / Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	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 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer3 filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* / Enable multicast traffic logging. *disable* / Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* / Enable sniffer traffic logging. *disable* / Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option / **Description** *enable* / Enable DLP archive logging. *disable* / Disable DLP archive logging.		
filter	FortiAnalyzer 3 log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer3 override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size
local-traffic	Enable/disable local in or out traffic logging.	option	-

Option	Description
enable	Enable local in or out traffic logging.

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option / **Description** *enable* / Enable multicast traffic logging. *disable* / Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option / **Description** *enable* / Enable sniffer traffic logging. *disable* / Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-
	Option / **Description** *enable* / Enable anomaly logging. *disable* / Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option / **Description** *enable* / Enable VoIP logging. *disable* / Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option / **Description** *enable* / Enable DLP archive logging. *disable* / Disable DLP archive logging.		
filter	FortiAnalyzer 3 log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option / **Description** *include* / Include logs that match the filter. *exclude* / 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 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
status	Enable/disable logging to FortiAnalyzer.	option	-

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	Disable logging to FortiAnalyzer.

Parameter	Description	Type	Size
ips-archive	Enable/disable IPS packet archive logging.	option	-

Option	Description
enable	Enable IPS packet archive logging.
disable	Disable IPS packet archive logging.

Parameter	Description	Type	Size
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-

Option	Description
enable	Enable FortiAnalyzer access to configuration and data.
disable	Disable FortiAnalyzer access to configuration and data.

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

Option	Description
sha256	Use SHA256 as HMAC algorithm.
sha1	Step down to SHA1 as the HMAC algorithm.

enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-

Option	Description
high-medium	Encrypt logs using high and medium encryption algorithms.
high	Encrypt logs using high encryption algorithms.
low	Encrypt logs using all encryption algorithms.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35

Parameter	Description	Type	Size
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	-

Option	Description
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.
realtime	Log directly to FortiAnalyzer in real time.
1-minute	Log directly to FortiAnalyzer at most every 1 minute.
5-minute	Log directly to FortiAnalyzer at most every 5 minutes.

upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-

Option	Description
daily	Upload log files to FortiAnalyzer once a day.
weekly	Upload log files to FortiAnalyzer once a week.
monthly	Upload log files to FortiAnalyzer once a month.

upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-time	Time to upload logs (hh:mm).	user	Not Specified
priority	Set log transmission priority.	option	-

Option	Description
default	Set FortiAnalyzer log transmission priority to default.
low	Set FortiAnalyzer log transmission priority to low.

max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

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 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
status	Enable/disable logging to FortiAnalyzer.	option	-

Option	Description
enable	Enable logging to FortiAnalyzer.
disable	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]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer-cloud filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.

Parameter	Description	Type	Size
	Option **Description** *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		

Parameter	Description	Type	Size
voip	Enable/disable VoIP logging.	option	-

Option	Description
enable	Enable VoIP logging.
disable	Disable VoIP logging.

Parameter	Description	Type	Size
dlp-archive	Enable/disable DLP archive logging.	option	-

Option	Description
enable	Enable DLP archive logging.
disable	Disable DLP archive logging.

Parameter	Description	Type	Size
filter	FortiAnalyzer Cloud log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud override-filter
   Description: Override filters for FortiAnalyzer Cloud.
   set severity [emergency|alert|...]
   set forward-traffic [enable|disable]
   set local-traffic [enable|disable]
   set multicast-traffic [enable|disable]
   set sniffer-traffic [enable|disable]
   set anomaly [enable|disable]
   set voip [enable|disable]
   set dlp-archive [enable|disable]
   set filter {string}
   set filter-type [include|exclude]
end
```

config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option **Description** *enable* Enable sniffer traffic logging. *disable* Disable sniffer traffic logging.		
anomaly	Enable/disable anomaly logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable anomaly logging. *disable* Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-
	Option **Description** *enable* Enable VoIP logging. *disable* Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option **Description** *enable* Enable DLP archive logging. *disable* Disable DLP archive logging.		
filter	FortiAnalyzer Cloud log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option **Description** *include* Include logs that match the filter. *exclude* Exclude logs that match the filter.		

mgmt-data

This section includes syntax for the following commands:

- config mgmt-data status on page 533

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 ospf6 on page 580
- config router bgp on page 593
- config router bfd on page 655
- config router ripng on page 552
- config router policy on page 560
- config router aspath-list on page 536
- config router static on page 557
- config router route-map on page 541
- config router info6 on page 654
- config router prefix-list6 on page 538
- config router ospf on page 566
- config router prefix-list on page 537
- config router rip on page 547
- config router access-list6 on page 535
- config router isis on page 630
- config router auth-path on page 654
- config router policy6 on page 563
- config router community-list on page 540
- config router info on page 653
- config router static6 on page 564
- config router multicast on page 644
- config router bfd6 on page 655
- config router access-list on page 534
- config router key-chain on page 539
- config router setting on page 654
- config router multicast6 on page 652
- config router multicast-flow on page 643

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]
            set flags {integer}
        next
    end
  next
end
```

config router access-list

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

config rule

Parameter	Description	Type	Size
action	Permit or deny this IP address and netmask prefix.	option	-

Option	Description
permit	Permit or allow this IP address and netmask prefix.
deny	Deny this IP address and netmask prefix.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable exact match.
disable	Disable exact match.

Parameter	Description	Type	Size
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295

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
comments	Comment.	string	Maximum length: 127

config rule

Parameter	Description	Type	Size
action	Permit or deny this IP address and netmask prefix.	option	-

Option	Description
permit	Permit or allow this IP address and netmask prefix.
deny	Deny this IP address and netmask prefix.

Parameter	Description	Type	Size
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified
exact-match	Enable/disable exact prefix match.	option	-

Option	Description
enable	Enable exact match.
disable	Disable exact match.

Parameter	Description	Type	Size
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295

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
action	Permit or deny route-based operations, based on the route's AS_PATH attribute.	option	-

Option	Description
deny	Deny route-based operations.
permit	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}
            set flags {integer}
         next
      end
   next
end
```

config router prefix-list

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

config rule

Parameter	Description	Type	Size
action	Permit or deny this IP address and netmask prefix.	option	-

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
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
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295

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
comments	Comment.	string	Maximum length: 127

config rule

Parameter	Description	Type	Size
action	Permit or deny packets that match this rule.	option	-

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

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 {string}
        next
     end
  next
end
```

config key

Parameter	Description	Type	Size
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. = 35 characters).	string	Maximum length: 35

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
type	Community list type (standard or expanded).	option	-

Option	Description
standard	Standard community list type.
expanded	Expanded community list type.

config rule

Parameter	Description	Type	Size
action	Permit or deny route-based operations, based on the route's COMMUNITY attribute.	option	-

Option	Description
deny	Deny route-based operations.
permit	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 [1|2|...]
            set match-tag {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 [1|2|...]
            set set-originator-id {ipv4-address-any}
            set set-origin [none|egp|...]
            set set-tag {integer}
            set set-weight {integer}
            set set-flags {integer}
            set match-flags {integer}
            set set-route-tag {integer}
        next
    end
  next
end
```

config router route-map

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

config rule

Parameter	Description	Type	Size
action	Action.	option	-

Option	Description
permit	Permit.
deny	Deny.

Parameter	Description	Type	Size
match-as-path	Match BGP AS path list.	string	Maximum length: 35
match-community	Match BGP community list.	string	Maximum length: 35
match-community-exact	Enable/disable exact matching of communities.	option	-

Option	Description
enable	Enable exact matching of communities.
disable	Disable exact matching of communities.

Parameter	Description	Type	Size
match-origin	Match BGP origin code.	option	-

Option	Description
none	None.
egp	Remote EGP.
igp	Local IGP.
incomplete	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
1	External type 1.
2	External type 2.
none	No type specified.

match-tag	Match tag.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
set-aggregator-as	BGP aggregator AS.	integer	Minimum value: 0 Maximum value: 4294967295
set-aggregator-ip	BGP aggregator IP.	ipv4-address-any	Not Specified
set-aspath-action	Specify preferred action of set-aspath.	option	-

Option	Description
prepend	Prepend.
replace	Replace.

set-aspath <as>	Prepend BGP AS path attribute. AS number (0 - 42949672). 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	-

Option	Description
enable	Enable BGP atomic aggregate attribute.
disable	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	-

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

Parameter	Description	Type	Size
set-dampening-reuse	Value to start reusing a route .	integer	Minimum value: 0 Maximum value: 20000
set-dampening-suppress	Value to start suppressing a route .	integer	Minimum value: 0 Maximum value: 20000
set-dampening-max-suppress	Maximum duration to suppress a route .	integer	Minimum value: 0 Maximum value: 255
set-dampening-unreachability-half-life	Unreachability Half-life time for the penalty	integer	Minimum value: 0 Maximum value: 45
set-extcommunity-rt <community>	Route Target extended community. AA:NN.	string	Maximum length: 79
set-extcommunity-soo <community>	Site-of-Origin extended community. 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
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	-

Parameter	Description	Type	Size
	Option **Description** *1* External type 1. *2* External type 2. *none* No type specified.		
set-originator-id	BGP originator ID attribute.	ipv4-address-any	Not Specified
set-origin	BGP origin code.	option	-
	Option **Description** *none* None. *egp* Remote EGP. *igp* Local IGP. *incomplete* 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-flags	BGP flags value	integer	Minimum value: 0 Maximum value: 65535
match-flags	BGP flag value to match	integer	Minimum value: 0 Maximum value: 65535
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-information-originate	Enable/disable generation of default route.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15
recv-buffer-size	Receiving buffer size.	integer	Minimum value: 8129 Maximum value: 2147483647
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79

Parameter	Description	Type	Size
update-timer	Update timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647
version	RIP version.	option	-

Option	Description
1	Version 1.
2	Version 2.

config distance

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

config distribute-list

Parameter	Description	Type	Size
status	status	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
direction	Distribute list direction.	option	-
	Option / **Description** *in* / Filter incoming packets. *out* / 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
ip	IP address.	ipv4-address	Not Specified

config network

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

config offset-list

Parameter	Description	Type	Size
status	status	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
direction	Offset list direction.	option	-
	Option / **Description** *in* / Filter incoming packets. *out* / Filter outgoing packets.		

Parameter	Description	Type	Size
access-list	Access list name.	string	Maximum length: 35
offset	offset	integer	Minimum value: 1 Maximum value: 16
interface	Interface name.	string	Maximum length: 15

config redistribute

Parameter	Description	Type	Size
status	status	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16
routemap	Route map name.	string	Maximum length: 35

config interface

Parameter	Description	Type	Size
auth-keychain	Authentication key-chain name.	string	Maximum length: 35
auth-mode	Authentication mode.	option	-

Option	Description
none	None.
text	Text.
md5	MD5.

auth-string	Authentication string/password.	password	Not Specified
receive-version	Receive version.	option	-

Parameter	Description	Type	Size
	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	-
	Option **Description** *disable* Disable broadcasting. *enable* Enable broadcasting.		
split-horizon-status	Enable/disable split horizon.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
split-horizon	Enable/disable split horizon.	option	-
	Option **Description** *poisoned* Poisoned. *regular* Regular.		
flags	flags	integer	Minimum value: 0 Maximum value: 255

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-information-originate	Enable/disable generation of default route.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79
update-timer	Update timer.	integer	Minimum value: 5 Maximum value: 2147483647
timeout-timer	Timeout timer.	integer	Minimum value: 5 Maximum value: 2147483647

Parameter	Description	Type	Size
garbage-timer	Garbage timer.	integer	Minimum value: 5 Maximum value: 2147483647

config distance

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

config distribute-list

Parameter	Description	Type	Size
status	status	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
direction	Distribute list direction.	option	-

Option	Description
in	Filter incoming packets.
out	Filter outgoing packets.

Parameter	Description	Type	Size
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
ip6	IPv6 link-local address.	ipv6-address	Not Specified

Parameter	Description	Type	Size
interface	Interface name.	string	Maximum length: 15

config network

Parameter	Description	Type	Size
prefix	Network IPv6 link-local prefix.	ipv6-prefix	Not Specified

config aggregate-address

Parameter	Description	Type	Size
prefix6	Aggregate address prefix.	ipv6-prefix	Not Specified

config offset-list

Parameter	Description	Type	Size
status	status	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
direction	Offset list direction.	option	-

Option	Description
in	Filter incoming packets.
out	Filter outgoing packets.

Parameter	Description	Type	Size
access-list6	IPv6 access list name.	string	Maximum length: 35
offset	offset	integer	Minimum value: 1 Maximum value: 16
interface	Interface name.	string	Maximum length: 15

config redistribute

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

config interface

Parameter	Description	Type	Size
split-horizon-status	Enable/disable split horizon.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
split-horizon	Enable/disable split horizon.	option	-
	Option / **Description** *poisoned* — Poisoned. *regular* — Regular.		
flags	Flags.	integer	Minimum value: 0 Maximum value: 255

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 virtual-wan-link [enable|disable]
      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
status	Enable/disable this static route.	option	-

Option	Description
enable	Enable static route.
disable	Disable static route.

dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified
src	Source prefix for this route.	ipv4-classnet	Not Specified
gateway	Gateway IP for this route.	ipv4-address	Not Specified
distance	Administrative distance .	integer	Minimum value: 1 Maximum value: 255
weight	Administrative weight .	integer	Minimum value: 0 Maximum value: 255
priority	Administrative priority .	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
device	Gateway out interface or tunnel.	string	Maximum length: 35
comment	Optional comments.	var-string	Maximum length: 255
blackhole	Enable/disable black hole.	option	-

Option	Description
enable	Enable black hole.
disable	Disable black hole.

dynamic-gateway	Enable use of dynamic gateway retrieved from a DHCP or PPP server.	option	-

Option	Description
enable	Enable dynamic gateway.
disable	Disable dynamic gateway.

virtual-wan-link	Enable/disable egress through the virtual-wan-link.	option	-

Option	Description
enable	Enable virtual-wan-link access.
disable	Disable virtual-wan-link access.

dstaddr	Name of firewall address or address group.	string	Maximum length: 79
internet-service	Application ID in the Internet service database.	integer	Minimum value: 0 Maximum value: 4294967295
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	-

Option	Description
enable	Enable withdrawal of this static route when link monitor or health check is down.

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable withdrawal of this static route when link monitor or health check is down.		
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-
	Option / **Description** *enable* / Enable Bidirectional Forwarding Detection (BFD). *disable* / 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
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79
input-device-negate	Enable/disable negation of input device match.	option	-

Option	Description
enable	Enable negation of input device match.
disable	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	-

Option	Description
enable	Enable source address negation.
disable	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	-

Option	Description
enable	Enable destination address negation.
disable	Disable destination address negation.

action	Action of the policy route.	option	-

Option	Description
deny	Do not search policy route table.
permit	Use this policy route for forwarding.

Parameter	Description	Type	Size
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255
start-port	Start destination port number .	integer	Minimum value: 0 Maximum value: 65535
end-port	End destination port number .	integer	Minimum value: 0 Maximum value: 65535
start-source-port	Start source port number .	integer	Minimum value: 0 Maximum value: 65535
end-source-port	End source port number .	integer	Minimum value: 0 Maximum value: 65535
gateway	IP address of the gateway.	ipv4-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	-

Option	Description
enable	Enable this policy route.
disable	Disable this policy route.

comments	Optional comments.	var-string	Maximum length: 255
internet-service-id `<id>`	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
internet-service-custom `<name>`	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79

config router 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
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79
src	Source IPv6 prefix.	ipv6-network	Not Specified
dst	Destination IPv6 prefix.	ipv6-network	Not Specified
protocol	Protocol number .	integer	Minimum value: 0 Maximum value: 255
start-port	Start destination port number .	integer	Minimum value: 1 Maximum value: 65535
end-port	End destination port number .	integer	Minimum value: 1 Maximum value: 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

Parameter	Description	Type	Size
tos-mask	Type of service evaluated bits.	user	Not Specified
status	Enable/disable this policy route.	option	-

Option	Description
enable	Enable this policy route.
disable	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 virtual-wan-link [enable|disable]
      set link-monitor-exempt [enable|disable]
      set bfd [enable|disable]
   next
end
```

config router static6

Parameter	Description	Type	Size
status	Enable/disable this static route.	option	-

Option	Description
enable	Enable static route.
disable	Disable static route.

dst	Destination IPv6 prefix.	ipv6-network	Not Specified
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified

Parameter	Description	Type	Size
device	Gateway out interface or tunnel.	string	Maximum length: 35
devindex	Device index .	integer	Minimum value: 0 Maximum value: 4294967295
distance	Administrative distance .	integer	Minimum value: 1 Maximum value: 255
priority	Administrative priority .	integer	Minimum value: 0 Maximum value: 4294967295
comment	Optional comments.	var-string	Maximum length: 255
blackhole	Enable/disable black hole.	option	-

Option	Description
enable	Enable black hole.
disable	Disable black hole.

virtual-wan-link	Enable/disable egress through the virtual-wan-link.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-

Option	Description
enable	Enable withdrawal of this static route when link monitor or health check is down.
disable	Disable withdrawal of this static route when link monitor or health check is down.

Parameter	Description	Type	Size
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-

Option	Description
enable	Enable Bidirectional Forwarding Detection (BFD).
disable	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]
         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 md5-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 interface {string}
         set ip {ipv4-address}
         set authentication [none|text|...]
         set authentication-key {password}
         set md5-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}
     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
abr-type	Area border router type.	option	-

Option	Description
cisco	Cisco.
ibm	IBM.
shortcut	Shortcut.
standard	Standard.

auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000
distance-external	Administrative external distance.	integer	Minimum value: 1 Maximum value: 255
distance-inter-area	Administrative inter-area distance.	integer	Minimum value: 1 Maximum value: 255
distance-intra-area	Administrative intra-area distance.	integer	Minimum value: 1 Maximum value: 255
database-overflow	Enable/disable database overflow.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

database-overflow-max-lsas	Database overflow maximum LSAs.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
database-overflow-time-to-recover	Database overflow time to recover (sec).	integer	Minimum value: 0 Maximum value: 65535
default-information-originate	Enable/disable generation of default route.	option	-

Option	Description
enable	Enable setting.
always	Always advertise the default router.
disable	Disable setting.

default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214
default-information-metric-type	Default information metric type.	option	-

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
distance	Distance of the route.	integer	Minimum value: 1 Maximum value: 255
rfc1583-compatible	Enable/disable RFC1583 compatibility.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
router-id	Router ID.	ipv4-address-any	Not Specified
spf-timers	SPF calculation frequency.	user	Not Specified
bfd	Bidirectional Forwarding Detection (BFD).	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
log-neighbour-changes	Enable logging of OSPF neighbour's changes	option	-
	Option **Description** *enable* Enable setting. *disable* 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	-
	Option **Description** *none* Hitless restart disabled. *lls* LLS mode. *graceful-restart* Graceful Restart Mode.		
restart-period	Graceful restart period.	integer	Minimum value: 1 Maximum value: 3600
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79

config area

Parameter	Description	Type	Size
shortcut	Enable/disable shortcut option.	option	-

Option	Description
disable	Disable shortcut option.
enable	Enable shortcut option.
default	Default shortcut option.

Parameter	Description	Type	Size
authentication	Authentication type.	option	-

Option	Description
none	None.
text	Text.
md5	MD5.

Parameter	Description	Type	Size
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 4294967295
nssa-translator-role	NSSA translator role type.	option	-

Option	Description
candidate	Candidate.
never	Never.
always	Always.

Parameter	Description	Type	Size
stub-type	Stub summary setting.	option	-

Option	Description
no-summary	No summary.
summary	Summary.

Parameter	Description	Type	Size
type	Area type setting.	option	-

Option	Description
regular	Regular.
nssa	NSSA.

Parameter	Description	Type	Size
	Option **Description** *stub* Stub.		
nssa-default-information-originate	Redistribute, advertise, or do not originate Type-7 default route into NSSA area.	option	-
	Option **Description** *enable* Redistribute Type-7 default route from routing table. *always* Advertise a self-originated Type-7 default route. *disable* Do not advertise Type-7 default route.		
nssa-default-information-originate-metric	OSPF default metric.	integer	Minimum value: 0 Maximum value: 16777214
nssa-default-information-originate-metric-type	OSPF metric type for default routes.	option	-
	Option **Description** *1* Type 1. *2* Type 2.		
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-
	Option **Description** *enable* Enable redistribute into NSSA area. *disable* Disable redistribute into NSSA area.		

config range

Parameter	Description	Type	Size
prefix	Prefix.	ipv4-classnet-any	Not Specified
advertise	Enable/disable advertise status.	option	-

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

config virtual-link

Parameter	Description	Type	Size
authentication	Authentication type.	option	-
	Option **Description** *none* None. *text* Text. *md5* MD5.		
authentication-key	Authentication key.	password	Not Specified
md5-keychain	Authentication MD5 key-chain name.	string	Maximum length: 35
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535

Parameter	Description	Type	Size
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535
peer	Peer IP.	ipv4-address-any	Not Specified

config md5-keys

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

config md5-keys

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

config filter-list

Parameter	Description	Type	Size
list	Access-list or prefix-list name.	string	Maximum length: 35
direction	Direction.	option	-

Option	Description
in	In.
out	Out.

config ospf-interface

Parameter	Description	Type	Size
interface	Configuration interface name.	string	Maximum length: 15
ip	IP address.	ipv4-address	Not Specified
authentication	Authentication type.	option	-

Parameter	Description	Type	Size
	Option **Description** *none* None. *text* Text. *md5* MD5.		
authentication-key	Authentication key.	password	Not Specified
md5-keychain	Authentication MD5 key-chain name.	string	Maximum length: 35
prefix-length	Prefix length.	integer	Minimum value: 0 Maximum value: 32
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535
priority	Priority.	integer	Minimum value: 0 Maximum value: 255
dead-interval	Dead interval.	integer	Minimum value: 0 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
hello-multiplier	Number of hello packets within dead interval.	integer	Minimum value: 3 Maximum value: 10
database-filter-out	Enable/disable control of flooding out LSAs.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
mtu	MTU for database description packets.	integer	Minimum value: 576 Maximum value: 65535
mtu-ignore	Enable/disable ignore MTU.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
network-type	Network type.	option	-

Option	Description
broadcast	Broadcast.
non-broadcast	Non-broadcast.
point-to-point	Point-to-point.
point-to-multipoint	Point-to-multipoint.
point-to-multipoint-non-broadcast	Point-to-multipoint and non-broadcast.

Parameter	Description	Type	Size
bfd	Bidirectional Forwarding Detection (BFD).	option	-

Option	Description
global	Follow global configuration.
enable	Enable BFD on this interface.
disable	Disable BFD on this interface.

Parameter	Description	Type	Size
status	Enable/disable status.	option	-
	Option / **Description** *disable* — Disable status. *enable* — Enable status.		
resync-timeout	Graceful restart neighbor resynchronization timeout.	integer	Minimum value: 1 Maximum value: 3600

config md5-keys

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

config md5-keys

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

config network

Parameter	Description	Type	Size
prefix	Prefix.	ipv4-classnet	Not Specified
area	Attach the network to area.	ipv4-address-any	Not Specified

config neighbor

Parameter	Description	Type	Size
ip	Interface IP address of the neighbor.	ipv4-address	Not Specified
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
priority	Priority.	integer	Minimum value: 0 Maximum value: 255

config summary-address

Parameter	Description	Type	Size
prefix	Prefix.	ipv4-classnet	Not Specified
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295
advertise	Enable/disable advertise status.	option	-

Option	Description
disable	Disable advertise status.
enable	Enable advertise status.

config distribute-list

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

Option	Description
connected	Connected type.
static	Static type.
rip	RIP type.

config redistribute

Parameter	Description	Type	Size
status	status	option	-

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

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
abr-type	Area border router type.	option	-

Parameter	Description	Type	Size
	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
default-information-originate	Enable/disable generation of default route.	option	-
	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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214
default-information-metric-type	Default information metric type.	option	-
	Option **Description** *1* Type 1. *2* Type 2.		

Parameter	Description	Type	Size
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
router-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified
spf-timers	SPF calculation frequency.	user	Not Specified
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-

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-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 16777215
nssa-translator-role	NSSA translator role type.	option	-

Option	Description
candidate	Candidate.
never	Never.
always	Always.

stub-type	Stub summary setting.	option	-

Parameter	Description	Type	Size
	Option / **Description** *no-summary* / No summary. *summary* / Summary.		
type	Area type setting.	option	-
	Option / **Description** *regular* / Regular. *nssa* / NSSA. *stub* / Stub.		
nssa-default-information-originate	Enable/disable originate type 7 default into NSSA area.	option	-
	Option / **Description** *enable* / Enable originate type 7 default into NSSA area. *disable* / Disable originate type 7 default into NSSA area.		
nssa-default-information-originate-metric	OSPFv3 default metric.	integer	Minimum value: 0 Maximum value: 16777214
nssa-default-information-originate-metric-type	OSPFv3 metric type for default routes.	option	-
	Option / **Description** *1* / Type 1. *2* / Type 2.		
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-
	Option / **Description** *enable* / Enable redistribute into NSSA area. *disable* / Disable redistribute into NSSA area.		
authentication	Authentication mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *none* — Disable authentication. *ah* — Authentication Header. *esp* — Encapsulating Security Payload.		
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000
ipsec-auth-alg	Authentication algorithm.	option	-
	Option / **Description** *md5* — MD5. *sha1* — SHA1. *sha256* — SHA256. *sha384* — SHA384. *sha512* — SHA512.		
ipsec-enc-alg	Encryption algorithm.	option	-
	Option / **Description** *null* — No encryption. *des* — DES. *3des* — 3DES. *aes128* — AES128. *aes192* — AES192. *aes256* — AES256.		

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified

config range

Parameter	Description	Type	Size
prefix6	IPv6 prefix.	ipv6-network	Not Specified
advertise	Enable/disable advertise status.	option	-

Option	Description
disable	disable
enable	enable

config virtual-link

Parameter	Description	Type	Size
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535
peer	A.B.C.D, peer router ID.	ipv4-address-any	Not Specified
authentication	Authentication mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *none* — Disable authentication. *ah* — Authentication Header. *esp* — Encapsulating Security Payload. *area* — Use the routing area's authentication configuration.		
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000
ipsec-auth-alg	Authentication algorithm.	option	-
	Option / **Description** *md5* — MD5. *sha1* — SHA1. *sha256* — SHA256. *sha384* — SHA384. *sha512* — SHA512.		
ipsec-enc-alg	Encryption algorithm.	option	-
	Option / **Description** *null* — No encryption. *des* — DES. *3des* — 3DES. *aes128* — AES128. *aes192* — AES192. *aes256* — AES256.		

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified

config ospf6-interface

Parameter	Description	Type	Size
area-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified
interface	Configuration interface name.	string	Maximum length: 15
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535
priority	priority	integer	Minimum value: 0 Maximum value: 255
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable OSPF6 routing on this interface.	option	-

Option	Description
disable	Disable OSPF6 routing.

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable OSPF6 routing.		
network-type	Network type.	option	-
	Option / **Description** *broadcast* / broadcast *point-to-point* / point-to-point *non-broadcast* / non-broadcast *point-to-multipoint* / point-to-multipoint *point-to-multipoint-non-broadcast* / point-to-multipoint and non-broadcast.		
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-
	Option / **Description** *global* / Use global configuration of Bidirectional Forwarding Detection (BFD). *enable* / Enable Bidirectional Forwarding Detection (BFD) on this interface. *disable* / Disable Bidirectional Forwarding Detection (BFD) on this interface.		
mtu	MTU for OSPFv3 packets.	integer	Minimum value: 576 Maximum value: 65535
mtu-ignore	Enable/disable ignoring MTU field in DBD packets.	option	-
	Option / **Description** *enable* / Ignore MTU field in DBD packets. *disable* / Do not ignore MTU field in DBD packets.		
authentication	Authentication mode.	option	-
	Option / **Description** *none* / Disable authentication. *ah* / Authentication Header. *esp* / Encapsulating Security Payload.		

Parameter	Description	Type	Size
	Option / **Description** *area* — Use the routing area's authentication configuration.		
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000
ipsec-auth-alg	Authentication algorithm.	option	-
	Option / **Description** *md5* — MD5. *sha1* — SHA1. *sha256* — SHA256. *sha384* — SHA384. *sha512* — SHA512.		
ipsec-enc-alg	Encryption algorithm.	option	-
	Option / **Description** *null* — No encryption. *des* — DES. *3des* — 3DES. *aes128* — AES128. *aes192* — AES192. *aes256* — AES256.		

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified

config neighbor

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

config redistribute

Parameter	Description	Type	Size
status	status	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214
routemap	Route map name.	string	Maximum length: 35
metric-type	Metric type.	option	-

Option	Description
1	Type 1.
2	Type 2.

config summary-address

Parameter	Description	Type	Size
prefix6	IPv6 prefix.	ipv6-network	Not Specified
advertise	Enable/disable advertise status.	option	-

Option	Description
disable	disable
enable	enable

tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295

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 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-multihop [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 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-multihop-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
   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-multihop [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 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-multihop-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
end
```

config router bgp

Parameter	Description	Type	Size
as	Router AS number, valid from 1 to 4294967295, 0 to disable BGP.	integer	Minimum value: 0 Maximum value: 4294967295
router-id	Router ID.	ipv4-address-any	Not Specified
keepalive-timer	Frequency to send keep alive requests.	integer	Minimum value: 0 Maximum value: 65535
holdtime-timer	Number of seconds to mark peer as dead.	integer	Minimum value: 3 Maximum value: 65535
always-compare-med	Enable/disable always compare MED.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
bestpath-as-path-ignore	Enable/disable ignore AS path.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
bestpath-cmp-confed-aspath	Enable/disable compare federation AS path length.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
bestpath-cmp-routerid	Enable/disable compare router ID for identical EBGP paths.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
bestpath-med-confed	Enable/disable compare MED among confederation paths.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
bestpath-med-missing-as-worst	Enable/disable treat missing MED as least preferred.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
client-to-client-reflection	Enable/disable client-to-client route reflection.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
dampening	Enable/disable route-flap dampening.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
deterministic-med	Enable/disable enforce deterministic comparison of MED.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ebgp-multipath	Enable/disable EBGP multi-path.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ibgp-multipath	Enable/disable IBGP multi-path.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
enforce-first-as	Enable/disable enforce first AS for EBGP routes.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
fast-external-failover	Enable/disable reset peer BGP session if link goes down.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
log-neighbour-changes	Enable logging of BGP neighbour's changes	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
network-import-check	Enable/disable ensure BGP network route exists in IGP.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ignore-optional-capability	Don't send unknown optional capability notification message	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
additional-path	Enable/disable selection of BGP IPv4 additional paths.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
additional-path6	Enable/disable selection of BGP IPv6 additional paths.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
cluster-id	Route reflector cluster ID.	ipv4-address-any	Not Specified
confederation-identifier	Confederation identifier.	integer	Minimum value: 1 Maximum value: 4294967295
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
dampening-reuse	Threshold to reuse routes.	integer	Minimum value: 1 Maximum value: 20000

Parameter	Description	Type	Size
dampening-suppress	Threshold to suppress routes.	integer	Minimum value: 1 Maximum value: 20000
dampening-max-suppress-time	Maximum minutes a route can be suppressed.	integer	Minimum value: 1 Maximum value: 255
dampening-unreachability-half-life	Unreachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45
default-local-preference	Default local preference.	integer	Minimum value: 0 Maximum value: 4294967295
scan-time	Background scanner interval (sec), 0 to disable it.	integer	Minimum value: 5 Maximum value: 60
distance-external	Distance for routes external to the AS.	integer	Minimum value: 1 Maximum value: 255
distance-internal	Distance for routes internal to the AS.	integer	Minimum value: 1 Maximum value: 255
distance-local	Distance for routes local to the AS.	integer	Minimum value: 1 Maximum value: 255
synchronization	Enable/disable only advertise routes from iBGP if routes present in an IGP.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

graceful-restart	Enable/disable BGP graceful restart capabilities.	option	-

Parameter	Description	Type	Size
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
graceful-restart-time	Time needed for neighbors to restart (sec).	integer	Minimum value: 1 Maximum value: 3600
graceful-stalepath-time	Time to hold stale paths of restarting neighbor (sec).	integer	Minimum value: 1 Maximum value: 3600
graceful-update-delay	Route advertisement/selection delay after restart (sec).	integer	Minimum value: 1 Maximum value: 3600
graceful-end-on-timer	Enable/disable to exit graceful restart on timer only.	option	-
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
additional-path-select	Number of additional paths to be selected for each IPv4 NLRI.	integer	Minimum value: 2 Maximum value: 4
additional-path-select6	Number of additional paths to be selected for each IPv6 NLRI.	integer	Minimum value: 2 Maximum value: 4

config aggregate-address

Parameter	Description	Type	Size
prefix	Aggregate prefix.	ipv4-classnet-any	Not Specified
as-set	Enable/disable generate AS set path information.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
summary-only	Enable/disable filter more specific routes from updates.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

config aggregate-address6

Parameter	Description	Type	Size
prefix6	Aggregate IPv6 prefix.	ipv6-prefix	Not Specified
as-set	Enable/disable generate AS set path information.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
summary-only	Enable/disable filter more specific routes from updates.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

config neighbor

Parameter	Description	Type	Size
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 1 Maximum value: 600
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-
	Option **Description** *as-path* AS path. *med* MED. *next-hop* Next hop.		
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-
	Option **Description** *as-path* AS path. *med* MED. *next-hop* Next hop.		
activate	Enable/disable address family IPv4 for this neighbor.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
bfd	Enable/disable BFD for this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-
	Option **Description** *none* None. *receive* Receive ORF lists. *send* Send ORF list. *both* Send and receive ORF lists.		
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-
	Option **Description** *none* None. *receive* Receive ORF lists. *send* Send ORF list. *both* Send and receive ORF lists.		

Parameter	Description	Type	Size
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGP neighbors.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
link-down-failover	Enable/disable failover upon link down.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
stale-route	Enable/disable stale route after neighbor down.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
override-capability	Enable/disable override result of capability negotiation.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
passive	Enable/disable sending of open messages to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-server-client	Enable/disable IPv4 AS route server client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-server-client6	Enable/disable IPv6 AS route server client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
shutdown	Enable/disable shutdown this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
strict-capability-match	Enable/disable strict capability matching.	option	-

Option	Description
enable	Enable setting.
disable	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
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 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

Parameter	Description	Type	Size
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295
maximum-prefix-threshold	Maximum IPv4 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35
route-map-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

Parameter	Description	Type	Size
send-community	IPv4 Send community attribute to neighbor.	option	-
	Option / **Description** *standard* — Standard. *extended* — Extended. *both* — Both. *disable* — Disable		
send-community6	IPv6 Send community attribute to neighbor.	option	-
	Option / **Description** *standard* — Standard. *extended* — Extended. *both* — Both. *disable* — Disable		
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535
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

Parameter	Description	Type	Size
restart-time	Graceful restart delay time .	integer	Minimum value: 0 Maximum value: 3600
additional-path	Enable/disable IPv4 additional-path capability.	option	-

Option	Description
send	Enable sending additional paths.
receive	Enable receiving additional paths.
both	Enable sending and receiving additional paths.
disable	Disable additional paths.

additional-path6	Enable/disable IPv6 additional-path capability.	option	-

Option	Description
send	Enable sending additional paths.
receive	Enable receiving additional paths.
both	Enable sending and receiving additional paths.
disable	Disable additional paths.

adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 4
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 4
password	Password used in MD5 authentication.	password	Not Specified

config conditional-advertise

Parameter	Description	Type	Size
condition-routemap	Name of condition route map.	string	Maximum length: 35
condition-type	Type of condition.	option	-

Option	Description
exist	True if condition route map is matched.
non-exist	True if condition route map is not matched.

config neighbor-group

Parameter	Description	Type	Size
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 1 Maximum value: 600
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-
	Option / **Description** *as-path* — AS path. *med* — MED. *next-hop* — Next hop.		
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-
	Option / **Description** *as-path* — AS path.		

Parameter	Description	Type	Size
	Option **Description** *med* MED. *next-hop* Next hop.		
activate	Enable/disable address family IPv4 for this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
bfd	Enable/disable BFD for this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-
	Option **Description** *none* None. *receive* Receive ORF lists. *send* Send ORF list. *both* Send and receive ORF lists.		
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-

Parameter	Description	Type	Size
	Option **Description** *none* None. *receive* Receive ORF lists. *send* Send ORF list. *both* Send and receive ORF lists.		
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

Parameter	Description	Type	Size
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGP neighbors.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
link-down-failover	Enable/disable failover upon link down.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
stale-route	Enable/disable stale route after neighbor down.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
override-capability	Enable/disable override result of capability negotiation.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
passive	Enable/disable sending of open messages to this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-server-client	Enable/disable IPv4 AS route server client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-server-client6	Enable/disable IPv6 AS route server client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
shutdown	Enable/disable shutdown this neighbor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
strict-capability-match	Enable/disable strict capability matching.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — 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
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 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

Parameter	Description	Type	Size
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
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295
maximum-prefix-threshold	Maximum IPv4 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value .	integer	Minimum value: 1 Maximum value: 100
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
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
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35
route-map-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

Parameter	Description	Type	Size
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	-

Option	Description
standard	Standard.
extended	Extended.
both	Both.
disable	Disable

Parameter	Description	Type	Size
send-community6	IPv6 Send community attribute to neighbor.	option	-

Option	Description
standard	Standard.
extended	Extended.
both	Both.
disable	Disable

Parameter	Description	Type	Size
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535
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

Parameter	Description	Type	Size
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535
restart-time	Graceful restart delay time .	integer	Minimum value: 0 Maximum value: 3600
additional-path	Enable/disable IPv4 additional-path capability.	option	-

Option	Description
send	Enable sending additional paths.
receive	Enable receiving additional paths.
both	Enable sending and receiving additional paths.
disable	Disable additional paths.

additional-path6	Enable/disable IPv6 additional-path capability.	option	-

Option	Description
send	Enable sending additional paths.
receive	Enable receiving additional paths.
both	Enable sending and receiving additional paths.
disable	Disable additional paths.

adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 4
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 4

config neighbor-range

Parameter	Description	Type	Size
prefix	Neighbor range prefix.	ipv4-classnet	Not Specified

Parameter	Description	Type	Size
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000
neighbor-group	Neighbor group name.	string	Maximum length: 63

config neighbor-range6

Parameter	Description	Type	Size
prefix6	IPv6 prefix.	ipv6-network	Not Specified
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000
neighbor-group	Neighbor group name.	string	Maximum length: 63

config network

Parameter	Description	Type	Size
prefix	Network prefix.	ipv4-classnet	Not Specified
backdoor	Enable/disable route as backdoor.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
route-map	Route map to modify generated route.	string	Maximum length: 35

config network6

Parameter	Description	Type	Size
prefix6	Network IPv6 prefix.	ipv6-network	Not Specified
backdoor	Enable/disable route as backdoor.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
route-map	Route map to modify generated route.	string	Maximum length: 35

config redistribute

Parameter	Description	Type	Size
status	Status	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
route-map	Route map name.	string	Maximum length: 35

config redistribute6

Parameter	Description	Type	Size
status	Status	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
route-map	Route map name.	string	Maximum length: 35

config admin-distance

Parameter	Description	Type	Size
neighbour-prefix	Neighbor address prefix.	ipv4-classnet	Not Specified
route-list	Access list of routes to apply new distance to.	string	Maximum length: 35

Parameter	Description	Type	Size
distance	Administrative distance to apply .	integer	Minimum value: 1 Maximum value: 255

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-l1 [password|md5]
   set auth-mode-l2 [password|md5]
   set auth-password-l1 {password}
   set auth-password-l2 {password}
   set auth-keychain-l1 {string}
   set auth-keychain-l2 {string}
   set auth-sendonly-l1 [enable|disable]
   set auth-sendonly-l2 [enable|disable]
   set ignore-lsp-errors [enable|disable]
   set lsp-gen-interval-l1 {integer}
   set lsp-gen-interval-l2 {integer}
   set lsp-refresh-interval {integer}
   set max-lsp-lifetime {integer}
   set spf-interval-exp-l1 {user}
   set spf-interval-exp-l2 {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-l1 [enable|disable]
   set redistribute-l1-list {string}
   set redistribute-l2 [enable|disable]
   set redistribute-l2-list {string}
   set redistribute6-l1 [enable|disable]
   set redistribute6-l1-list {string}
   set redistribute6-l2 [enable|disable]
   set redistribute6-l2-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
is-type	IS type.	option	-

Option	Description
level-1-2	Level 1 and 2.
level-1	Level 1 only.
level-2-only	Level 2 only.

Parameter	Description	Type	Size
adv-passive-only	Enable/disable IS-IS advertisement of passive interfaces only.	option	-

Option	Description
enable	Advertise passive interfaces only.
disable	Advertise all IS-IS enabled interfaces.

Parameter	Description	Type	Size
adv-passive-only6	Enable/disable IPv6 IS-IS advertisement of passive interfaces only.	option	-

Option	Description
enable	Advertise passive interfaces only.
disable	Advertise all IS-IS enabled interfaces.

Parameter	Description	Type	Size
auth-mode-l1	Level 1 authentication mode.	option	-

Option	Description
password	Password.
md5	MD5.

Parameter	Description	Type	Size
auth-mode-l2	Level 2 authentication mode.	option	-

Parameter	Description	Type	Size
	Option **Description** *password* Password. *md5* 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	-
	Option **Description** *enable* Enable level 1 authentication send-only. *disable* Disable level 1 authentication send-only.		
auth-sendonly-l2	Enable/disable level 2 authentication send-only.	option	-
	Option **Description** *enable* Enable level 2 authentication send-only. *disable* Disable level 2 authentication send-only.		
ignore-lsp-errors	Enable/disable ignoring of LSP errors with bad checksums.	option	-
	Option **Description** *enable* Enable ignoring of LSP errors with bad checksums. *disable* 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

Parameter	Description	Type	Size
lsp-gen-interval-l2	Minimum interval for level 2 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120
lsp-refresh-interval	LSP refresh time in seconds.	integer	Minimum value: 1 Maximum value: 65535
max-lsp-lifetime	Maximum LSP lifetime in seconds.	integer	Minimum value: 350 Maximum value: 65535
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	-

Option	Description
enable	Enable dynamic hostname.
disable	Disable dynamic hostname.

adjacency-check	Enable/disable adjacency check.	option	-

Option	Description
enable	Enable adjacency check.
disable	Disable adjacency check.

adjacency-check6	Enable/disable IPv6 adjacency check.	option	-

Option	Description
enable	Enable IPv6 adjacency check.
disable	Disable IPv6 adjacency check.

overload-bit	Enable/disable signal other routers not to use us in SPF.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable overload bit. *disable* / Disable overload bit.		
overload-bit-suppress	Suppress overload-bit for the specific prefixes.	option	-
	Option / **Description** *external* / External. *interlevel* / Inter-level.		
overload-bit-on-startup	Overload-bit only temporarily after reboot.	integer	Minimum value: 5 Maximum value: 86400
default-originate	Enable/disable distribution of default route information.	option	-
	Option / **Description** *enable* / Enable distribution of default route information. *disable* / Disable distribution of default route information.		
default-originate6	Enable/disable distribution of default IPv6 route information.	option	-
	Option / **Description** *enable* / Enable distribution of default IPv6 route information. *disable* / Disable distribution of default IPv6 route information.		
metric-style	Use old-style (ISO 10589) or new-style packet formats	option	-
	Option / **Description** *narrow* / Use old style of TLVs with narrow metric. *wide* / Use new style of TLVs to carry wider metric. *transition* / Send and accept both styles of TLVs during transition. *narrow-transition* / Narrow and accept both styles of TLVs during transition.		

Parameter	Description	Type	Size
	Option / **Description** *narrow-transition-l1* / Narrow-transition level-1 only. *narrow-transition-l2* / Narrow-transition level-2 only. *wide-l1* / Wide level-1 only. *wide-l2* / Wide level-2 only. *wide-transition* / Wide and accept both styles of TLVs during transition. *wide-transition-l1* / Wide-transition level-1 only. *wide-transition-l2* / Wide-transition level-2 only. *transition-l1* / Transition level-1 only. *transition-l2* / Transition level-2 only.		
redistribute-l1	Enable/disable redistribution of level 1 routes into level 2.	option	-
	Option / **Description** *enable* / Enable redistribution of level 1 routes into level 2. *disable* / 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	-
	Option / **Description** *enable* / Enable redistribution of level 2 routes into level 1. *disable* / 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	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable redistribution of level 1 IPv6 routes into level 2. *disable* Disable redistribution of level 1 IPv6 routes into level 2.		
redistribute6-l1-list	Access-list for IPv6 route redistribution from l1 to l2.	string	Maximum length: 35
redistribute6-l2	Enable/disable redistribution of level 2 IPv6 routes into level 1.	option	-
	Option **Description** *enable* Enable redistribution of level 2 IPv6 routes into level 1. *disable* Disable redistribution of level 2 IPv6 routes into level 1.		
redistribute6-l2-list	Access-list for IPv6 route redistribution from l2 to l1.	string	Maximum length: 35

config isis-net

Parameter	Description	Type	Size
net	IS-IS net xx.xxxx. … .xxxx.xx.	user	Not Specified

config isis-interface

Parameter	Description	Type	Size
status	Enable/disable interface for IS-IS.	option	-
	Option **Description** *enable* Enable interface for IS-IS. *disable* Disable interface for IS-IS.		
status6	Enable/disable IPv6 interface for IS-IS.	option	-
	Option **Description** *enable* Enable IPv6 interface for IS-IS. *disable* Disable IPv6 interface for IS-IS.		
network-type	IS-IS interface's network type	option	-

Parameter	Description	Type	Size
	Option / **Description** *broadcast* / Broadcast. *point-to-point* / Point-to-point. *loopback* / Loopback.		
circuit-type	IS-IS interface's circuit type	option	-
	Option / **Description** *level-1-2* / Level 1 and 2. *level-1* / Level 1. *level-2* / Level 2.		
csnp-interval-l1	Level 1 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535
csnp-interval-l2	Level 2 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval-l1	Level 1 hello interval.	integer	Minimum value: 0 Maximum value: 65535
hello-interval-l2	Level 2 hello interval.	integer	Minimum value: 0 Maximum value: 65535
hello-multiplier-l1	Level 1 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100
hello-multiplier-l2	Level 2 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100
hello-padding	Enable/disable padding to IS-IS hello packets.	option	-

Parameter	Description	Type	Size
	Option: *enable* — Enable padding to IS-IS hello packets. Option: *disable* — Disable padding to IS-IS hello packets.		
lsp-interval	LSP transmission interval (milliseconds).	integer	Minimum value: 1 Maximum value: 4294967295
lsp-retransmit-interval	LSP retransmission interval (sec).	integer	Minimum value: 1 Maximum value: 65535
metric-l1	Level 1 metric for interface.	integer	Minimum value: 1 Maximum value: 63
metric-l2	Level 2 metric for interface.	integer	Minimum value: 1 Maximum value: 63
wide-metric-l1	Level 1 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214
wide-metric-l2	Level 2 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214
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
auth-send-only-l1	Enable/disable authentication send-only for level 1 PDUs.	option	-

Option	Description
enable	Enable authentication send-only for level 1 PDUs.
disable	Disable authentication send-only for level 1 PDUs.

Parameter	Description	Type	Size
auth-send-only-l2	Enable/disable authentication send-only for level 2 PDUs.	option	-

Option	Description
enable	Enable authentication send-only for level 2 PDUs.
disable	Disable authentication send-only for level 2 PDUs.

Parameter	Description	Type	Size
auth-mode-l1	Level 1 authentication mode.	option	-

Option	Description
md5	MD5.
password	Password.

Parameter	Description	Type	Size
auth-mode-l2	Level 2 authentication mode.	option	-

Option	Description
md5	MD5.
password	Password.

Parameter	Description	Type	Size
priority-l1	Level 1 priority.	integer	Minimum value: 0 Maximum value: 127
priority-l2	Level 2 priority.	integer	Minimum value: 0 Maximum value: 127
mesh-group	Enable/disable IS-IS mesh group.	option	-

Option	Description
enable	Enable IS-IS mesh group.
disable	Disable IS-IS mesh group.

Parameter	Description	Type	Size
mesh-group-id	Mesh group ID <0-4294967295>, 0: mesh-group blocked.	integer	Minimum value: 0 Maximum value: 4294967295

config summary-address

Parameter	Description	Type	Size
prefix	Prefix.	ipv4-classnet-any	Not Specified
level	Level.	option	-

Option	Description
level-1-2	Level 1 and 2.
level-1	Level 1.
level-2	Level 2.

config summary-address6

Parameter	Description	Type	Size
prefix6	IPv6 prefix.	ipv6-prefix	Not Specified
level	Level.	option	-

Option	Description
level-1-2	Level 1 and 2.
level-1	Level 1.
level-2	Level 2.

config redistribute

Parameter	Description	Type	Size
status	Status.	option	-

Option	Description
enable	Enable.
disable	Disable.

Parameter	Description	Type	Size
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864
metric-type	Metric type.	option	-

Option	Description
external	External.
internal	Internal.

level	Level.	option	-

Option	Description
level-1-2	Level 1 and 2.
level-1	Level 1.
level-2	Level 2.

routemap	Route map name.	string	Maximum length: 35

config redistribute6

Parameter	Description	Type	Size
status	Enable/disable redistribution.	option	-

Option	Description
enable	Enable redistribution.
disable	Disable redistribution.

metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864
metric-type	Metric type.	option	-

Option	Description
external	External metric type.
internal	Internal metric type.

Parameter	Description	Type	Size
level	Level.	option	-
	Option / **Description** *level-1-2* — Level 1 and 2. *level-1* — Level 1. *level-2* — 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
comments	Comment.	string	Maximum length: 127

config flows

Parameter	Description	Type	Size
group-addr	Multicast group IP address.	ipv4-address-any	Not Specified
source-addr	Multicast source IP address.	ipv4-address-any	Not Specified

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
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
route-limit	Maximum number of multicast routes.	integer	Minimum value: 1 Maximum value: 2147483647
multicast-routing	Enable/disable IP multicast routing.	option	-

Option	Description
enable	Enable IP multicast routing.
disable	Disable IP multicast routing.

config pim-sm-global

Parameter	Description	Type	Size
message-interval	Period of time between sending periodic PIM join/prune messages in seconds .	integer	Minimum value: 1 Maximum value: 65535
join-prune-holdtime	Join/prune holdtime .	integer	Minimum value: 1 Maximum value: 65535
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	-

Option	Description
enable	Allow this router to function as a BSR.
disable	Do not allow this router to function as a BSR.

bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15
bsr-priority	BSR priority .	integer	Minimum value: 0 Maximum value: 255
bsr-hash	BSR hash length .	integer	Minimum value: 0 Maximum value: 32
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-

Option	Description
enable	Allow quick refresh packets.
disable	Do not allow quick refresh packets.

cisco-register-checksum	Checksum entire register packet(for old Cisco IOS compatibility).	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / register checksum entire packet. *disable* / 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	-
	Option / **Description** *enable* / Do not allow sending group prefix of zero. *disable* / Allow sending group prefix of zero.		
cisco-ignore-rp-set-priority	Use only hash for RP selection (compatibility with old Cisco IOS).	option	-
	Option / **Description** *enable* / Ignore RP-SET priority value. *disable* / Do not ignore RP-SET priority value.		
register-rp-reachability	Enable/disable check RP is reachable before registering packets.	option	-
	Option / **Description** *enable* / Check target RP is unicast reachable before registering. *disable* / Do not check RP unicast reachability.		
register-source	Override source address in register packets.	option	-
	Option / **Description** *disable* / Use source address of RPF interface. *interface* / Use primary IP of an interface. *ip-address* / 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

Parameter	Description	Type	Size
register-supression	Period of time to honor register-stop message .	integer	Minimum value: 1 Maximum value: 65535
null-register-retries	Maximum retries of null register .	integer	Minimum value: 1 Maximum value: 20
rp-register-keepalive	Timeout for RP receiving data on .	integer	Minimum value: 1 Maximum value: 65535
spt-threshold	Enable/disable switching to source specific trees.	option	-

Option	Description
enable	Switch to Source tree when available.
disable	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	-

Option	Description
enable	Allow source specific multicast.
disable	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

config rp-address

Parameter	Description	Type	Size
ip-address	RP router address.	ipv4-address	Not Specified
group	Groups to use this RP.	string	Maximum length: 35

config interface

Parameter	Description	Type	Size
ttl-threshold	Minimum TTL of multicast packets that will be forwarded .	integer	Minimum value: 1 Maximum value: 255
pim-mode	PIM operation mode.	option	-

Option	Description
sparse-mode	sparse-mode
dense-mode	dense-mode

Parameter	Description	Type	Size
passive	Enable/disable listening to IGMP but not participating in PIM.	option	-

Option	Description
enable	Listen only.
disable	Participate in PIM.

Parameter	Description	Type	Size
bfd	Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	option	-

Option	Description
enable	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).
disable	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).

Parameter	Description	Type	Size
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
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	-

Parameter	Description	Type	Size
	Option: *enable* — Description: Do not send GenID. Option: *disable* — Description: Send GenID according to standard.		
dr-priority	DR election priority.	integer	Minimum value: 1 Maximum value: 4294967295
propagation-delay	Delay flooding packets on this interface .	integer	Minimum value: 100 Maximum value: 5000
state-refresh-interval	Interval between sending state-refresh packets .	integer	Minimum value: 1 Maximum value: 100
rp-candidate	Enable/disable compete to become RP in elections.	option	-
	Option: *enable* — Description: Compete for RP elections. Option: *disable* — Description: 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
rp-candidate-interval	RP candidate advertisement interval .	integer	Minimum value: 1 Maximum value: 16383
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	-

Parameter	Description	Type	Size
	Option: *enable* — Enable fail back for RPF neighbor query. Option: *disable* — 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
access-group	Groups IGMP hosts are allowed to join.	string	Maximum length: 35
version	Maximum version of IGMP to support. Option: *3* — Version 3 and lower. Option: *2* — Version 2 and lower. Option: *1* — Version 1.	option	-
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
last-member-query-count	Number of group specific queries before removing group .	integer	Minimum value: 2 Maximum value: 7
query-max-response-time	Maximum time to wait for a IGMP query response .	integer	Minimum value: 1 Maximum value: 25
query-interval	Interval between queries to IGMP hosts .	integer	Minimum value: 1 Maximum value: 65535

Parameter	Description	Type	Size
query-timeout	Timeout between queries before becoming querier for network .	integer	Minimum value: 60 Maximum value: 900
router-alert-check	Enable/disable require IGMP packets contain router alert option.	option	-

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-holdtime {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 {ipv6-address}
         next
      end
   end
end
```

config router multicast6

Parameter	Description	Type	Size
multicast-routing	Enable/disable IPv6 multicast routing.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable IPv6 multicast routing. *disable* / Disable IPv6 multicast routing.		
multicast-pmtu	Enable/disable PMTU for IPv6 multicast.	option	-
	Option / **Description** *enable* / Enable PMTU for IPv6 multicast. *disable* / Disable PMTU for IPv6 multicast.		

config interface

Parameter	Description	Type	Size
hello-interval	Interval between sending PIM hello messages ..	integer	Minimum value: 1 Maximum value: 65535
hello-holdtime	Time before old neighbour information expires .	integer	Minimum value: 1 Maximum value: 65535

config pim-sm-global

Parameter	Description	Type	Size
register-rate-limit	Limit of packets/sec per source registered through this RP (0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535

config rp-address

Parameter	Description	Type	Size
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
device	Outgoing interface.	string	Maximum length: 35
gateway	Gateway IP address.	ipv4-address	Not Specified

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
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
```

config neighbor

Parameter	Description	Type	Size
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
interface	Interface to the BFD neighbor.	string	Maximum length: 15

ssh-filter

This section includes syntax for the following commands:

- config ssh-filter profile on page 656

config ssh-filter profile

SSH filter profile.

```
config ssh-filter profile
   Description: 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
      config file-filter
         Description: File filter.
         set status [enable|disable]
         set log [enable|disable]
         set scan-archive-contents [enable|disable]
         config entries
            Description: File filter entries.
            edit <filter>
               set comment {var-string}
               set action [log|block]
               set direction [incoming|outgoing|...]
               set password-protected [yes|any]
               set file-type <name1>, <name2>, ...
            next
         end
      end
   next
end
```

config ssh-filter profile

Parameter	Description	Type	Size
block	SSH blocking options.	option	-

Option	Description
x11	X server forwarding.
shell	SSH shell.
exec	SSH execution.
port-forward	Port forwarding.
tun-forward	Tunnel forwarding.
sftp	SFTP.
scp	SCP.
unknown	Unknown channel.

Parameter	Description	Type	Size
log	SSH logging options.	option	-

Option	Description
x11	X server forwarding.
shell	SSH shell.
exec	SSH execution.
port-forward	Port forwarding.
tun-forward	Tunnel forwarding.
sftp	SFTP.
scp	SCP.
unknown	Unknown channel.

Parameter	Description	Type	Size
default-command-log	Enable/disable logging unmatched shell commands.	option	-

Option	Description
enable	Enable log unmatched shell commands.
disable	Disable log unmatched shell commands.

config shell-commands

Parameter	Description	Type	Size
type	Matching type.	option	-
	Option / **Description** *simple* — Match single command. *regex* — Match command line using regular expression.		
pattern	SSH shell command pattern.	string	Maximum length: 128
action	Action to take for URL filter matches.	option	-
	Option / **Description** *block* — Block the SSH shell command. *allow* — Allow the SSH shell command.		
log	Enable/disable logging.	option	-
	Option / **Description** *enable* — Enable logging. *disable* — Disable logging.		
alert	Enable/disable alert.	option	-
	Option / **Description** *enable* — Enable alert. *disable* — Disable alert.		
severity	Log severity.	option	-
	Option / **Description** *low* — Severity low. *medium* — Severity medium. *high* — Severity high. *critical* — Severity critical.		

config file-filter

Parameter	Description	Type	Size
status	Enable/disable file filter.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable file filter. *disable* Disable file filter.		
log	Enable/disable file filter logging.	option	-
	Option **Description** *enable* Enable file filter logging. *disable* Disable file filter logging.		
scan-archive-contents	Enable/disable file filter archive contents scan.	option	-
	Option **Description** *enable* Enable file filter archive contents scan. *disable* Disable file filter archive contents scan.		

config entries

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
action	Action taken for matched file.	option	-
	Option **Description** *log* Allow the content and write a log message. *block* Block the content and write a log message.		
direction	Match files transmitted in the session's originating or reply direction.	option	-
	Option **Description** *incoming* Match files transmitted in the session's originating direction. *outgoing* Match files transmitted in the session's reply direction. *any* Match files transmitted in the session's originating and reply direction.		
password-protected	Match password-protected files.	option	-

Parameter	Description	Type	Size
	Option / **Description** *yes* / Match only password-protected files. *any* / Match any file.		
file-type <name>	Select file type. File type name.	string	Maximum length: 39

switch-controller

This section includes syntax for the following commands:

- config switch-controller flow-tracking on page 725
- config switch-controller security-policy local-access on page 666
- config switch-controller switch-profile on page 686
- config switch-controller security-policy 802-1X on page 664
- config switch-controller qos qos-policy on page 682
- config switch-controller network-monitor-settings on page 724
- config switch-controller system on page 720
- config switch-controller global on page 718
- config switch-controller auto-config custom on page 686
- config switch-controller switch-interface-tag on page 663
- config switch-controller stp-instance on page 716
- config switch-controller qos queue-policy on page 680
- config switch-controller lldp-profile on page 672
- config switch-controller auto-config policy on page 684
- config switch-controller lldp-settings on page 671
- config switch-controller switch-log on page 721
- config switch-controller poe on page 721
- config switch-controller 802-1X-settings on page 663
- config switch-controller remote-log on page 734
- config switch-controller switch-group on page 715
- config switch-controller stp-settings on page 715
- config switch-controller virtual-port-pool on page 687
- config switch-controller location on page 667
- config switch-controller custom-command on page 687
- config switch-controller qos ip-dscp-map on page 679
- config switch-controller snmp-trap-threshold on page 728
- config switch-controller storm-control on page 717
- config switch-controller sflow on page 723
- config switch-controller snmp-sysinfo on page 727
- config switch-controller traffic-policy on page 662
- config switch-controller snmp-user on page 731
- config switch-controller traffic-sniffer on page 732
- config switch-controller qos dot1p-map on page 675
- config switch-controller snmp-community on page 729
- config switch-controller auto-config default on page 685
- config switch-controller storm-control-policy on page 683
- config switch-controller quarantine on page 723
- config switch-controller igmp-snooping on page 722
- config switch-controller managed-switch on page 688

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
description	Description of the traffic policy.	string	Maximum length: 63
policer-status	Enable/disable policer config on the traffic policy.	option	-

Option	Description
enable	Enable policer config on the traffic policy.
disable	Disable policer config on the traffic policy.

guaranteed-bandwidth	Guaranteed bandwidth in kbps (max value = 524287000).	integer	Minimum value: 0 Maximum value: 524287000
guaranteed-burst	Guaranteed burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
maximum-burst	Maximum burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
type	Configure type of policy(ingress/egress).	option	-

Parameter	Description	Type	Size
	Option / **Description** *ingress* / Ingress policy. *egress* / Egress policy.		
cos-queue	COS queue, or unset to disable.	integer	Minimum value: 0 Maximum value: 7

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}
end
```

config switch-controller 802-1X-settings

Parameter	Description	Type	Size
link-down-auth	Interface-reauthentication state to set if a link is down.	option	-
	Option / **Description** *set-unauth* / Interface set to unauth when down. Reauthentication is needed. *no-action* / Interface reauthentication is not needed.		

Parameter	Description	Type	Size
reauth-period	Period of time to allow for reauthentication .	integer	Minimum value: 0 Maximum value: 1440
max-reauth-attempt	Maximum number of authentication attempts .	integer	Minimum value: 0 Maximum value: 15

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 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}
   next
end
```

config switch-controller security-policy 802-1X

Parameter	Description	Type	Size
security-mode	Port or MAC based 802.1X security mode.	option	-

Option	Description
802.1X	802.1X port based authentication.
802.1X-mac-based	802.1X MAC based authentication.

Parameter	Description	Type	Size
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
mac-auth-bypass	Enable/disable MAB for this policy.	option	-

Option	Description
disable	Disable MAB.
enable	Enable MAB.

Parameter	Description	Type	Size
open-auth	Enable/disable open authentication for this policy.	option	-

Option	Description
disable	Disable open authentication.
enable	Enable open authentication.

Parameter	Description	Type	Size
eap-passthru	Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for more flexible authentication.	option	-

Option	Description
disable	Disable EAP pass-through mode on this interface.
enable	Enable EAP pass-through mode on this interface.

Parameter	Description	Type	Size
guest-vlan	Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.	option	-

Option	Description
disable	Disable guest VLAN on this interface.
enable	Enable guest VLAN on this interface.

Parameter	Description	Type	Size
guest-vlan-id	Guest VLAN name.	string	Maximum length: 15
guest-auth-delay	Guest authentication delay .	integer	Minimum value: 1 Maximum value: 900
auth-fail-vlan	Enable to allow limited access to clients that cannot authenticate.	option	-

Option	Description
disable	Disable authentication fail VLAN on this interface.
enable	Enable authentication fail VLAN on this interface.

Parameter	Description	Type	Size
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	-

Option	Description
disable	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.
enable	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.

Parameter	Description	Type	Size
radius-timeout-overwrite	Enable to override the global RADIUS session timeout.	option	-

Option	Description
disable	Override the global RADIUS session timeout.
enable	Use the global RADIUS session timeout.

Parameter	Description	Type	Size
policy-type	Policy type.	option	-

Option	Description
802.1X	802.1X security policy.

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
mgmt-allowaccess	Allowed access on the switch management interface.	option	-

Parameter	Description	Type	Size
	Option / **Description** *https* — HTTPS access. *ping* — PING access. *ssh* — SSH access. *snmp* — SNMP access. *http* — HTTP access. *telnet* — TELNET access. *radius-acct* — RADIUS accounting access.		
internal-allowaccess	Allowed access on the switch internal interface.	option	-
	Option / **Description** *https* — HTTPS access. *ping* — PING access. *ssh* — SSH access. *snmp* — SNMP access. *http* — HTTP access. *telnet* — TELNET access. *radius-acct* — 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
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

Parameter	Description	Type	Size
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
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

Parameter	Description	Type	Size
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
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
altitude	+/- Floating point no. eg. 117.47.	string	Maximum length: 15
altitude-unit	m (meters), f (floors).	option	-

Option	Description
m	set altitude unit meters
f	set altitude unit floors

datum	WGS84, NAD83, NAD83/MLLW.	option	-

Parameter	Description	Type	Size
	Option / **Description** *WGS84* / set coordinates datum WGS84 *NAD83* / set coordinates datum NAD83 *NAD83/MLLW* / 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
elin-num	Configure ELIN callback number.	string	Maximum length: 31
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]
end
```

config switch-controller lldp-settings

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
tx-interval	Frequency of LLDP PDU transmission from FortiSwitch . Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 5 Maximum value: 4095
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
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	option	-

Option	Description
internal	Use internal interface.
mgmt	Use management interface.

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}
      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
med-tlvs	Transmitted LLDP-MED TLVs (type-length-value descriptions).	option	-

Option	Description
inventory-management	Inventory management TLVs.
network-policy	Network policy TLVs.
power-management	Power manangement TLVs.
location-identification	Location identificaion TLVs.

Parameter	Description	Type	Size
802 1-tlvs	Transmitted IEEE 802.1 TLVs.	option	-

Option	Description
port-vlan-id	Port native VLAN TLV.

Parameter	Description	Type	Size
802 3-tlvs	Transmitted IEEE 802.3 TLVs.	option	-

Option	Description
max-frame-size	Maximum frame size TLV.
power-negotiation	PoE+ classification TLV.

Parameter	Description	Type	Size
auto-isl	Enable/disable auto inter-switch LAG.	option	-

Option	Description
disable	Disable auto inter-switch-LAG.
enable	Enable auto inter-switch-LAG.

Parameter	Description	Type	Size
auto-isl-hello-timer	Auto inter-switch LAG hello timer duration .	integer	Minimum value: 1 Maximum value: 30
auto-isl-receive-timeout	Auto inter-switch LAG timeout if no response is received .	integer	Minimum value: 0 Maximum value: 90
auto-isl-port-group	Auto inter-switch LAG port group ID .	integer	Minimum value: 0 Maximum value: 9

config med-network-policy

Parameter	Description	Type	Size
status	Enable or disable this TLV.	option	-

Option	Description
disable	Do not transmit this network policy TLV.
enable	Transmit this TLV if a VLAN has been addded 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	-

Option	Description
disable	Disable VLAN assignment when this profile is applied on port.
enable	Enable VLAN assignment when this profile is applied on port.

priority	Advertised Layer 2 priority .	integer	Minimum value: 0 Maximum value: 7
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

config med-location-service

Parameter	Description	Type	Size
status	Enable or disable this TLV.	option	-
	Option / **Description** *disable* — Do not transmit this location service TLV. *enable* — Transmit this location service TLV.		
sys-location-id	Location service ID.	string	Maximum length: 63

config custom-tlvs

Parameter	Description	Type	Size
oui	Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.	user	Not Specified
subtype	Organizationally defined subtype .	integer	Minimum value: 0 Maximum value: 255
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
description	Description of the 802.1p name.	string	Maximum length: 63
egress-pri-tagging	Enable/disable egress priority-tag frame.	option	-

Option	Description
disable	Disable egress priority tagging.
enable	Enable egress priority tagging.

Parameter	Description	Type	Size
priority-0	COS queue mapped to dot1p priority number.	option	-

Option	Description
queue-0	COS queue 0 (lowest priority).
queue-1	COS queue 1.
queue-2	COS queue 2.
queue-3	COS queue 3.
queue-4	COS queue 4.
queue-5	COS queue 5.
queue-6	COS queue 6.
queue-7	COS queue 7 (highest priority).

Parameter	Description	Type	Size
priority-1	COS queue mapped to dot1p priority number.	option	-

Option	Description
queue-0	COS queue 0 (lowest priority).
queue-1	COS queue 1.
queue-2	COS queue 2.
queue-3	COS queue 3.
queue-4	COS queue 4.
queue-5	COS queue 5.
queue-6	COS queue 6.
queue-7	COS queue 7 (highest priority).

Parameter	Description	Type	Size
priority-2	COS queue mapped to dot1p priority number.	option	-

Parameter	Description	Type	Size
	Option / **Description** *queue-0* — COS queue 0 (lowest priority). *queue-1* — COS queue 1. *queue-2* — COS queue 2. *queue-3* — COS queue 3. *queue-4* — COS queue 4. *queue-5* — COS queue 5. *queue-6* — COS queue 6. *queue-7* — COS queue 7 (highest priority).		
priority-3	COS queue mapped to dot1p priority number.	option	-
	Option / **Description** *queue-0* — COS queue 0 (lowest priority). *queue-1* — COS queue 1. *queue-2* — COS queue 2. *queue-3* — COS queue 3. *queue-4* — COS queue 4. *queue-5* — COS queue 5. *queue-6* — COS queue 6. *queue-7* — COS queue 7 (highest priority).		
priority-4	COS queue mapped to dot1p priority number.	option	-
	Option / **Description** *queue-0* — COS queue 0 (lowest priority). *queue-1* — COS queue 1. *queue-2* — COS queue 2. *queue-3* — COS queue 3. *queue-4* — COS queue 4. *queue-5* — COS queue 5. *queue-6* — COS queue 6. *queue-7* — COS queue 7 (highest priority).		

Parameter	Description	Type	Size
priority-5	COS queue mapped to dot1p priority number.	option	-

Option	Description
queue-0	COS queue 0 (lowest priority).
queue-1	COS queue 1.
queue-2	COS queue 2.
queue-3	COS queue 3.
queue-4	COS queue 4.
queue-5	COS queue 5.
queue-6	COS queue 6.
queue-7	COS queue 7 (highest priority).

priority-6	COS queue mapped to dot1p priority number.	option	-

Option	Description
queue-0	COS queue 0 (lowest priority).
queue-1	COS queue 1.
queue-2	COS queue 2.
queue-3	COS queue 3.
queue-4	COS queue 4.
queue-5	COS queue 5.
queue-6	COS queue 6.
queue-7	COS queue 7 (highest priority).

priority-7	COS queue mapped to dot1p priority number.	option	-

Option	Description
queue-0	COS queue 0 (lowest priority).
queue-1	COS queue 1.
queue-2	COS queue 2.
queue-3	COS queue 3.
queue-4	COS queue 4.
queue-5	COS queue 5.
queue-6	COS queue 6.
queue-7	COS queue 7 (highest priority).

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
description	Description of the ip-dscp map name.	string	Maximum length: 63

config map

Parameter	Description	Type	Size
cos-queue	COS queue number.	integer	Minimum value: 0 Maximum value: 7
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
	Option / **Description** *AF22* / DSCP AF22. *AF23* / DSCP AF23. *CS3* / DSCP CS3. *AF31* / DSCP AF31. *AF32* / DSCP AF32. *AF33* / DSCP AF33. *CS4* / DSCP CS4. *AF41* / DSCP AF41. *AF42* / DSCP AF42. *AF43* / DSCP AF43. *CS5* / DSCP CS5. *EF* / DSCP EF. *CS6* / DSCP CS6. *CS7* / DSCP CS7.		
ip-precedence	IP Precedence.	option	-
	Option / **Description** *network-control* / Network control. *internetwork-control* / Internetwork control. *critic-ecp* / Critic ECP. *flashoverride* / Flash override. *flash* / Flash. *immediate* / Immediate. *priority* / Priority. *routine* / Routine.		
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 weight {integer}
         next
      end
   next
end
```

config switch-controller qos queue-policy

Parameter	Description	Type	Size
schedule	COS queue scheduling.	option	-

Option	Description
strict	Strict scheduling (queue7: highest priority, queue0: lowest priority).
round-robin	Round robin scheduling.
weighted	Weighted round robin scheduling.

Parameter	Description	Type	Size
rate-by	COS queue rate by kbps or percent.	option	-

Option	Description
kbps	Rate by kbps.
percent	Rate by percent.

config cos-queue

Parameter	Description	Type	Size
description	Description of the COS queue.	string	Maximum length: 63
min-rate	Minimum rate .	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
max-rate	Maximum rate .	integer	Minimum value: 0 Maximum value: 4294967295
min-rate-percent	Minimum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295
max-rate-percent	Maximum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295
drop-policy	COS queue drop policy.	option	-

Option	Description
taildrop	Taildrop policy.
weighted-random-early-detection	Weighted random early detection drop policy.

weight	Weight of weighted round robin scheduling.	integer	Minimum value: 0 Maximum value: 4294967295

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-cos	Default cos queue for untagged packets.	integer	Minimum value: 0 Maximum value: 7
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

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
description	Description of the storm control policy.	string	Maximum length: 63
storm-control-mode	Set Storm control mode.	option	-

Option	Description
global	Apply Global or switch level storm control configuration.
override	Override global and switch level storm control to use port level configuration.

Parameter	Description	Type	Size
	Option / **Description** *disabled* / Disable storm control on the port entirely overriding global and switch level storm control.		
rate	Threshold rate in packets per second at which storm traffic is controlled in override mode .	integer	Minimum value: 0 Maximum value: 10000000
unknown-unicast	Enable/disable storm control to drop/allow unknown unicast traffic in override mode.	option	-
	Option / **Description** *enable* / Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits. *disable* / 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	-
	Option / **Description** *enable* / Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits. *disable* / 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	-
	Option / **Description** *enable* / Enable storm control for broadcast traffic to drop packets which exceed configured rate limits. *disable* / 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
qos-policy	Auto-Config QoS policy.	string	Maximum length: 63
storm-control-policy	Auto-Config storm control policy.	string	Maximum length: 63
poe-status	Enable/disable PoE status.	option	-

Option	Description
enable	Enable PoE status.
disable	Disable PoE status.

Parameter	Description	Type	Size
igmp-flood-report	Enable/disable IGMP flood report.	option	-

Option	Description
enable	Enable IGMP flood report.
disable	Disable IGMP flood report.

Parameter	Description	Type	Size
igmp-flood-traffic	Enable/disable IGMP flood traffic.	option	-

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
fgt-policy	Default FortiLink auto-config policy.	string	Maximum length: 63
isl-policy	Default ISL auto-config policy.	string	Maximum length: 63
icl-policy	Default ICL auto-config policy.	string	Maximum length: 63

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
policy	Custom auto-config policy.	string	Maximum length: 63

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
login-passwd-override	Enable/disable overriding the admin administrator password for a managed FortiSwitch with the FortiGate admin administrator account password.	option	-

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
description	Description.	string	Maximum length: 35
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
description	Virtual switch pool description.	string	Maximum length: 63

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 poe-detection-type {integer}
      set poe-lldp-detection [enable|disable]
      set directly-connected {integer}
      set version {integer}
      set pre-provisioned {integer}
      set dynamic-capability {integer}
      set switch-device-tag {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}
      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 poe-pre-standard-detection [enable|disable]
            set port-number {integer}
            set port-prefix-type {integer}
            set fortilink-port {integer}
            set poe-capable {integer}
            set stacking-port {integer}
            set fiber-port {integer}
            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 dhcp-snooping [untrusted|trusted]
      set dhcp-snoop-option82-trust [enable|disable]
      set arp-inspection-trust [untrusted|trusted]
      set igmp-snooping [enable|disable]
      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 loop-guard [enabled|disabled]
      set loop-guard-timeout {integer}
      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 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|sha]
      set auth-pwd {password}
      set priv-proto [aes|des]
      set priv-pwd {password}
   next
end
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}
     end
  next
end
```

config switch-controller managed-switch

Parameter	Description	Type	Size
name	Managed-switch name.	string	Maximum length: 35
description	Description.	string	Maximum length: 63
switch-profile	FortiSwitch profile.	string	Maximum length: 35
access-profile	FortiSwitch access profile.	string	Maximum length: 31
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	-

Option	Description
discovered	Link waiting to be authorized.
disable	Link unauthorized.
enable	Link authorized.

poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable PoE pre-standard detection. *disable* Disable PoE pre-standard detection.		
poe-detection-type	PoE detection type for FortiSwitch.	integer	Minimum value: 0 Maximum value: 255
poe-lldp-detection	Enable/disable PoE LLDP detection.	option	-
	Option **Description** *enable* Enable PoE LLDP detection. *disable* Disable PoE LLDP detection.		
directly-connected	Directly connected FortiSwitch.	integer	Minimum value: 0 Maximum value: 1
version	FortiSwitch version.	integer	Minimum value: 0 Maximum value: 255
pre-provisioned	Pre-provisioned managed switch.	integer	Minimum value: 0 Maximum value: 255
dynamic-capability	List of features this FortiSwitch supports (not configurable) that is sent to the FortiGate device for subsequent configuration initiated by the FortiGate device.	integer	Minimum value: 0 Maximum value: 4294967295
switch-device-tag	User definable label/tag.	string	Maximum length: 32
mclag-igmp-snooping-aware	Enable/disable MCLAG IGMP-snooping awareness.	option	-
	Option **Description** *enable* Enable MCLAG IGMP-snooping awareness.		

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable MCLAG IGMP-snooping awareness.		
dynamically-discovered	Dynamically discovered FortiSwitch.	integer	Minimum value: 0 Maximum value: 1
type	Indication of switch type, physical or virtual.	option	-
	Option / **Description** *virtual* / Switch is of type virtual. *physical* / Switch is of type physical.		
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
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
override-snmp-sysinfo	Enable/disable overriding the global SNMP system information.	option	-
	Option / **Description** *disable* / Use the global SNMP system information. *enable* / Override the global SNMP system information.		
override-snmp-trap-threshold	Enable/disable overriding the global SNMP trap threshold values.	option	-
	Option / **Description** *enable* / Override the global SNMP trap threshold values. *disable* / Use the global SNMP trap threshold values.		
override-snmp-community	Enable/disable overriding the global SNMP communities.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Override the global SNMP communities. *disable* / Use the global SNMP communities.		
override-snmp-user	Enable/disable overriding the global SNMP users.	option	-
	Option / **Description** *enable* / Override the global SNMPv3 users. *disable* / Use the global SNMPv3 users.		

config ports

Parameter	Description	Type	Size
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	-
	Option / **Description** *10half* / 10M half-duplex. *10full* / 10M full-duplex. *100half* / 100M half-duplex. *100full* / 100M full-duplex. *1000auto* / Auto-negotiation (1G full-duplex only). *1000fiber* / 1G full-duplex (fiber SFPs only) *1000full* / 1G full-duplex *10000* / 10G full-duplex *40000* / 40G full-duplex *auto* / Auto-negotiation. *auto-module* / Auto Module. *100FX-half* / 100Mbps half-duplex.100Base-FX.		

Parameter	Description	Type	Size
	Option / **Description** *100FX-full* — 100Mbps full-duplex. 100Base-FX. *100000full* — 100Gbps full-duplex. *2500auto* — Auto-Negotiation (2.5Gbps Only). *25000full* — 25Gbps full-duplex. *50000full* — 50Gbps full-duplex. *10000cr* — 10Gbps copper interface. *10000sr* — 10Gbps SFI interface. *100000sr4* — 100Gbps SFI interface. *100000cr4* — 100Gbps copper interface. *25000cr4* — 25Gbps copper interface. *25000sr4* — 25Gbps SFI interface. *5000full* — 5Gbps full-duplex.		
status	Switch port admin status: up or down.	option	-
	Option / **Description** *up* — Set admin status up. *down* — Set admin status down.		
poe-status	Enable/disable PoE status.	option	-
	Option / **Description** *enable* — Enable PoE status. *disable* — Disable PoE status.		
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-
	Option / **Description** *enable* — Enable PoE pre-standard detection. *disable* — Disable PoE pre-standard detection.		

Parameter	Description	Type	Size
port-number	Port number.	integer	Minimum value: 1 Maximum value: 64
port-prefix-type	Port prefix type.	integer	Minimum value: 0 Maximum value: 1
fortilink-port	FortiLink uplink port.	integer	Minimum value: 0 Maximum value: 1
poe-capable	PoE capable.	integer	Minimum value: 0 Maximum value: 1
stacking-port	Stacking port.	integer	Minimum value: 0 Maximum value: 1
fiber-port	Fiber-port.	integer	Minimum value: 0 Maximum value: 1
flags	Port properties flags.	integer	Minimum value: 0 Maximum value: 4294967295
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

Parameter	Description	Type	Size
vlan	Assign switch ports to a VLAN.	string	Maximum length: 15
allowed-vlans-all	Enable/disable all defined vlans on this port.	option	-

Option	Description
enable	Enable all defined VLANs on this port.
disable	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	-

Option	Description
physical	Physical port.
trunk	Trunk port.

dhcp-snooping	Trusted or untrusted DHCP-snooping interface.	option	-

Option	Description
untrusted	Untrusted DHCP snooping interface.
trusted	Trusted DHCP snooping interface.

dhcp-snoop-option82-trust	Enable/disable allowance of DHCP with option-82 on untrusted interface.	option	-

Option	Description
enable	Enable allowance of DHCP with option-82 on untrusted interface.
disable	Disable allowance of DHCP with option-82 on untrusted interface.

arp-inspection-trust	Trusted or untrusted dynamic ARP inspection.	option	-

Option	Description
untrusted	Untrusted dynamic ARP inspection.
trusted	Trusted dynamic ARP inspection.

Parameter	Description	Type	Size
igmp-snooping	Set IGMP snooping mode for the physical port interface.	option	-

Option	Description
enable	Interface takes part in IGMP snooping.
disable	Interface does not take part in IGMP snooping.

Parameter	Description	Type	Size
igmps-flood-reports	Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.	option	-

Option	Description
enable	Enable flooding of IGMP snooping reports to this interface.
disable	Disable flooding of IGMP snooping reports to this interface.

Parameter	Description	Type	Size
igmps-flood-traffic	Enable/disable flooding of IGMP snooping traffic to this interface.	option	-

Option	Description
enable	Enable flooding of IGMP snooping traffic to this interface.
disable	Disable flooding of IGMP snooping traffic to this interface.

Parameter	Description	Type	Size
stp-state	Enable/disable Spanning Tree Protocol (STP) on this interface.	option	-

Option	Description
enabled	Enable STP on this interface.
disabled	Disable STP on this interface.

Parameter	Description	Type	Size
stp-root-guard	Enable/disable STP root guard on this interface.	option	-

Option	Description
enabled	Enable STP root-guard on this interface.
disabled	Disable STP root-guard on this interface.

Parameter	Description	Type	Size
stp-bpdu-guard	Enable/disable STP BPDU guard on this interface.	option	-

Option	Description
enabled	Enable STP BPDU guard on this interface.
disabled	Disable STP BPDU guard on this interface.

Parameter	Description	Type	Size
stp-bpdu-guard-timeout	BPDU Guard disabling protection .	integer	Minimum value: 0 Maximum value: 120
edge-port	Enable/disable this interface as an edge port, bridging connections between workstations and/or computers.	option	-

Option	Description
enable	Enable this interface as an edge port.
disable	Disable this interface as an edge port.

discard-mode	Configure discard mode for port.	option	-

Option	Description
none	Discard disabled.
all-untagged	Discard all frames that are untagged.
all-tagged	Discard all frames that are tagged.

packet-sampler	Enable/disable packet sampling on this interface.	option	-

Option	Description
enabled	Enable packet sampling on this interface.
disabled	Disable packet sampling on this interface.

packet-sample-rate	Packet sampling rate .	integer	Minimum value: 0 Maximum value: 99999
sflow-counter-interval	sFlow sampling counter polling interval .	integer	Minimum value: 0 Maximum value: 255
sample-direction	Packet sampling direction.	option	-

Option	Description
tx	Monitor transmitted traffic.
rx	Monitor received traffic.

Parameter	Description	Type	Size
	Option **Description** *both* Monitor transmitted and received traffic.		
loop-guard	Enable/disable loop-guard on this interface, an STP optimization used to prevent network loops.	option	-
	Option **Description** *enabled* Enable loop-guard on this interface. *disabled* Disable loop-guard on this interface.		
loop-guard-timeout	Loop-guard timeout .	integer	Minimum value: 0 Maximum value: 120
qos-policy	Switch controller QoS policy from available options.	string	Maximum length: 63
storm-control-policy	Switch controller storm control policy from available options.	string	Maximum length: 63
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 pool. FortiSwitch port tag name when exported to a virtual pool.	string	Maximum length: 63
learning-limit	Limit the number of dynamic MAC addresses on this Port .	integer	Minimum value: 0 Maximum value: 128
sticky-mac	Enable or disable sticky-mac on the interface.	option	-
	Option **Description** *enable* Enable sticky mac on the interface. *disable* Disable sticky mac on the interface.		
lldp-status	LLDP transmit and receive status.	option	-

Parameter	Description	Type	Size
	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
export-to	Export managed-switch port to a tenant VDOM.	string	Maximum length: 31
mac-addr	Port/Trunk MAC.	mac-address	Not Specified
port-selection-criteria	Algorithm for aggregate port selection.	option	-
	Option / **Description** *src-mac* / Source MAC address. *dst-mac* / Destination MAC address. *src-dst-mac* / Source and destination MAC address. *src-ip* / Source IP address. *dst-ip* / Destination IP address. *src-dst-ip* / Source and destination IP address.		
description	Description for port.	string	Maximum length: 63
lacp-speed	end Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second (fast).	option	-
	Option / **Description** *slow* / Send LACP message every 30 seconds. *fast* / Send LACP message every second.		
mode	LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.	option	-

Parameter	Description	Type	Size
	Option / **Description** *static* — Static aggregation, do not send and ignore any control messages. *lacp-passive* — Passively use LACP to negotiate 802.3ad aggregation. *lacp-active* — Actively use LACP to negotiate 802.3ad aggregation.		
bundle	Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.	option	-
	Option / **Description** *enable* — Enable bundling. *disable* — Disable bundling.		
member-withdrawal-behavior	Port behavior after it withdraws because of loss of control packets.	option	-
	Option / **Description** *forward* — Forward traffic. *block* — Block traffic.		
mclag	Enable/disable multi-chassis link aggregation (MCLAG).	option	-
	Option / **Description** *enable* — Enable MCLAG. *disable* — Disable MCLAG.		
min-bundle	Minimum size of LAG bundle	integer	Minimum value: 1 Maximum value: 24
max-bundle	Maximum size of LAG bundle	integer	Minimum value: 1 Maximum value: 24
members <member-name>	Aggregated LAG bundle interfaces. Interface name from available options.	string	Maximum length: 79

config stp-settings

Parameter	Description	Type	Size
local-override	Enable to configure local STP settings that override global STP settings.	option	-

Option	Description
enable	Override global STP settings.
disable	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
hello-time	Period of time between successive STP frame Bridge Protocol Data Units .	integer	Minimum value: 1 Maximum value: 10
forward-time	Period of time a port is in listening and learning state .	integer	Minimum value: 4 Maximum value: 30
max-age	Maximum time before a bridge port saves its configuration BPDU information .	integer	Minimum value: 6 Maximum value: 40
max-hops	Maximum number of hops between the root bridge and the furthest bridge .	integer	Minimum value: 1 Maximum value: 40
pending-timer	Pending time .	integer	Minimum value: 1 Maximum value: 15

config stp-instance

Parameter	Description	Type	Size
priority	Priority.	option	-

Parameter	Description	Type	Size

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
status	Enable/disable SNMP.	option	-

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
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295

config snmp-community

Parameter	Description	Type	Size
name	SNMP community name.	string	Maximum length: 35
status	Enable/disable this SNMP community.	option	-

Option	Description
disable	Disable SNMP community.
enable	Enable SNMP community.

Parameter	Description	Type	Size
query-v1-status	Enable/disable SNMP v1 queries.	option	-

Option	Description
disable	Disable SNMP v1 queries.
enable	Enable SNMP v1 queries.

Parameter	Description	Type	Size
query-v1-port	SNMP v1 query port .	integer	Minimum value: 0 Maximum value: 65535
query-v2c-status	Enable/disable SNMP v2c queries.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable SNMP v2c queries. *enable* Enable SNMP v2c queries.		
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535
trap-v1-status	Enable/disable SNMP v1 traps.	option	-
	Option **Description** *disable* Disable SNMP v1 traps. *enable* Enable SNMP v1 traps.		
trap-v1-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535
trap-v1-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-
	Option **Description** *disable* Disable SNMP v2c traps. *enable* Enable SNMP v2c traps.		
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535
events	SNMP notifications (traps) to send.	option	-

Parameter	Description	Type	Size

Option	Description
cpu-high	Send a trap when CPU usage too high.
mem-low	Send a trap when available memory is low.
log-full	Send a trap when log disk space becomes low.
intf-ip	Send a trap when an interface IP address is changed.
ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).

config hosts

Parameter	Description	Type	Size
ip	IPv4 address of the SNMP manager (host).	user	Not Specified

config snmp-user

Parameter	Description	Type	Size
queries	Enable/disable SNMP queries for this user.	option	-

Option	Description
disable	Disable SNMP queries for this user.
enable	Enable SNMP queries for this user.

query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535
security-level	Security level for message authentication and encryption.	option	-

Option	Description
no-auth-no-priv	Message with no authentication and no privacy (encryption).
auth-no-priv	Message with authentication but no privacy (encryption).
auth-priv	Message with authentication and privacy (encryption).

auth-proto	Authentication protocol.	option	-

Option	Description
md5	HMAC-MD5-96 authentication protocol.
sha	HMAC-SHA-96 authentication protocol.

Parameter	Description	Type	Size
auth-pwd	Password for authentication protocol.	password	Not Specified
priv-proto	Privacy (encryption) protocol.	option	-

Option	Description
aes	CFB128-AES-128 symmetric encryption protocol.
des	CBC-DES symmetric encryption protocol.

Parameter	Description	Type	Size
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified

config switch-log

Parameter	Description	Type	Size
local-override	Enable to configure local logging settings that override global logging settings.	option	-

Option	Description
enable	Override global logging settings.
disable	Use global logging settings.

Parameter	Description	Type	Size
status	Enable/disable adding FortiSwitch logs to the FortiGate event log.	option	-

Option	Description
enable	Add FortiSwitch logs to the FortiGate event log.
disable	Do not add FortiSwitch logs to the FortiGate event log.

Parameter	Description	Type	Size
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

config remote-log

Parameter	Description	Type	Size
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-

Option	Description
enable	Enable logging by FortiSwitch device to a remote syslog server.
disable	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
severity	Severity of logs to be transferred to remote log server.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

csv	Enable/disable comma-separated value (CSV) strings.	option	-

Option	Description
enable	Enable comma-separated value (CSV) strings.
disable	Disable comma-separated value (CSV) strings.

facility	Facility to log to remote syslog server.	option	-

Option	Description
kernel	Kernel messages.

Parameter	Description	Type	Size

Option	Description
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslogd.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	UUCP server messages.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

config storm-control

Parameter	Description	Type	Size
local-override	Enable to override global FortiSwitch storm control settings for this FortiSwitch.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Override global storm control settings. *disable* — 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
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-
	Option / **Description** *enable* — Drop unknown unicast traffic. *disable* — Allow unknown unicast traffic.		
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-
	Option / **Description** *enable* — Drop unknown multicast traffic. *disable* — Allow unknown multicast traffic.		
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-
	Option / **Description** *enable* — Drop broadcast traffic. *disable* — Allow broadcast traffic.		

config mirror

Parameter	Description	Type	Size
status	Active/inactive mirror configuration.	option	-
	Option / **Description** *active* — Activate mirror configuration. *inactive* — Deactivate mirror configuration.		
switching-packet	Enable/disable switching functionality when mirroring.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable switching functionality when mirroring. *disable* — 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
type	Type.	option	-
	Option / **Description** *static* — Static MAC. *sticky* — Sticky MAC.		
vlan	Vlan.	string	Maximum length: 15
mac	MAC address.	mac-address	Not Specified
interface	Interface name.	string	Maximum length: 35
description	Description.	string	Maximum length: 63

config custom-command

Parameter	Description	Type	Size
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
local-override	Enable/disable overriding the global IGMP snooping configuration.	option	-

Option	Description
enable	Override the global IGMP snooping configuration.
disable	Use the global IGMP snooping configuration.

Parameter	Description	Type	Size
aging-time	Maximum time to retain a multicast snooping entry for which no packets have been seen .	integer	Minimum value: 15 Maximum value: 3600
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-

Option	Description
enable	Enable unknown multicast flooding.
disable	Disable unknown multicast flooding.

config 802-1X-settings

Parameter	Description	Type	Size
local-override	Enable to override global 802.1X settings on individual FortiSwitches.	option	-

Option	Description
enable	Override global 802.1X settings.
disable	Use global 802.1X settings.

Parameter	Description	Type	Size
link-down-auth	Authentication state to set if a link is down.	option	-

Option	Description
set-unauth	Interface set to unauth when down. Reauthentication is needed.
no-action	Interface reauthentication is not needed.

Parameter	Description	Type	Size
reauth-period	Reauthentication time interval .	integer	Minimum value: 0 Maximum value: 1440

Parameter	Description	Type	Size
max-reauth-attempt	Maximum number of authentication attempts .	integer	Minimum value: 0 Maximum value: 15

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 members <name1>, <name2>, ...
   next
end
```

config switch-controller switch-group

Parameter	Description	Type	Size
description	Optional switch group description.	string	Maximum length: 63
members <name>	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
name	Name of global STP settings configuration.	string	Maximum length: 31
revision	STP revision number .	integer	Minimum value: 0 Maximum value: 65535
hello-time	Period of time between successive STP frame Bridge Protocol Data Units .	integer	Minimum value: 1 Maximum value: 10
forward-time	Period of time a port is in listening and learning state .	integer	Minimum value: 4 Maximum value: 30
max-age	Maximum time before a bridge port saves its configuration BPDU information .	integer	Minimum value: 6 Maximum value: 40
max-hops	Maximum number of hops between the root bridge and the furthest bridge .	integer	Minimum value: 1 Maximum value: 40
pending-timer	Pending time .	integer	Minimum value: 1 Maximum value: 15

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
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
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
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-

Option	Description
enable	Enable unknown unicast storm control.
disable	Disable unknown unicast storm control.

Parameter	Description	Type	Size
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-

Option	Description
enable	Enable unknown multicast storm control.
disable	Disable unknown multicast storm control.

Parameter	Description	Type	Size
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-

Parameter	Description	Type	Size

Option	Description
enable	Enable broadcast storm control.
disable	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 allow-multiple-interfaces [enable|disable]
   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 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]
   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
end
```

config switch-controller global

Parameter	Description	Type	Size
mac-aging-interval	Time after which an inactive MAC is aged out .	integer	Minimum value: 10 Maximum value: 1000000
allow-multiple-interfaces	Enable/disable multiple FortiLink interfaces for redundant connections between a managed FortiSwitch and FortiGate.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable FortiLink on multiple interfaces. *disable* Disable FortiLink on multiple interfaces.		
https-image-push	Enable/disable image push to FortiSwitch using HTTPS.	option	-
	Option **Description** *enable* Enable image push to FortiSwitch using HTTPS. *disable* Disable image push to FortiSwitch using HTTPS.		
vlan-all-mode	VLAN configuration mode, user-defined-vlans or all-possible-vlans.	option	-
	Option **Description** *all* Include all possible VLANs (1-4093). *defined* Include user defined VLANs.		
vlan-optimization	FortiLink VLAN optimization.	option	-
	Option **Description** *enable* Enable VLAN optimization on FortiSwitch units for auto-generated trunks. *disable* 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
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
default-virtual-switch-vlan	Default VLAN for ports when added to the virtual-switch.	string	Maximum length: 15
log-mac-limit-violations	Enable/disable logs for Learning Limit Violations.	option	-
	Option **Description** *enable* Enable Learn Limit Violation. *disable* Disable Learn Limit Violation.		

Parameter	Description	Type	Size
mac-violation-timer	Set timeout for Learning Limit Violations (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295
sn-dns-resolution	Enable/disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	option	-

Option	Description
enable	Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.
disable	Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.

Parameter	Description	Type	Size
mac-event-logging	Enable/disable MAC address event logging.	option	-

Option	Description
enable	Enable MAC address event logging.
disable	Disable MAC address event logging.

Parameter	Description	Type	Size
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	-

Option	Description
disable	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.
enable	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.

config custom-command

Parameter	Description	Type	Size
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}
end
```

config switch-controller system

Parameter	Description	Type	Size
parallel-process-override	Enable/disable parallel process override.	option	-
	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: 300
data-sync-interval	Time interval between collection of switch data .	integer	Minimum value: 30 Maximum value: 1800

config switch-controller poe

List PoE end-points status.

```
config switch-controller poe
   Description: List PoE end-points status.
   set <fortiswitch-id> {string}
end
```

config switch-controller poe

Parameter	Description	Type	Size
<fortiswitch-id>	FortiSwitch device ID.	string	Maximum length: -1

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
status	Enable/disable adding FortiSwitch logs to FortiGate event log.	option	-

Option	Description
enable	Add FortiSwitch logs to FortiGate event log.
disable	Do not add FortiSwitch logs to FortiGate event log.

Parameter	Description	Type	Size
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

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
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
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-

Option	Description
enable	Enable unknown multicast flooding.
disable	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
collector-ip	Collector IP.	ipv4-address	Not Specified
collector-port	SFlow collector port .	integer	Minimum value: 0 Maximum value: 65535

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
quarantine	Enable/disable quarantine.	option	-

Option	Description
enable	Enable quarantine.
disable	Disable quarantine.

config targets

Parameter	Description	Type	Size
description	Description for the quarantine MAC.	string	Maximum length: 63
tag <tags>	Tags for the quarantine MAC. Tag string(eg. 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
network-monitoring	Enable/disable passive gathering of information by FortiSwitch units concerning other network devices.	option	-

Option	Description
enable	Enable network monitoring on FortiSwitch.
disable	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
sample-mode	Configure sample mode for the flow tracking.	option	-

Option	Description
local	Set local mode which samples on the specific switch port.
perimeter	Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.
device-ingress	Set device -ingress mode which samples across all switch ports at the ingress.

sample-rate	Configure sample rate for the perimeter and device-ingress sampling.	integer	Minimum value: 0 Maximum value: 99999
format	Configure flow tracking protocol.	option	-

Parameter	Description	Type	Size
	Option / **Description** *netflow1* / Netflow version 1 sampling. *netflow5* / Netflow version 5 sampling. *netflow9* / Netflow version 9 sampling. *ipfix* / Ipfix sampling.		
collector-ip	Configure collector ip address.	ipv4-address	Not Specified
collector-port	Configure collector port number.	integer	Minimum value: 0 Maximum value: 65535
transport	Configure L4 transport protocol for exporting packets.	option	-
	Option / **Description** *udp* / UDP protocol. *tcp* / TCP protocol. *sctp* / SCTP protocol.		
level	Configure flow tracking level.	option	-
	Option / **Description** *vlan* / Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet. *ip* / Collects srcip/dstip from the sample packet. *port* / Collects srcip/dstip/srcport/dstport/protocol from the sample packet. *proto* / Collects srcip/dstip/protocol from the sample packet. *mac* / Collects smac/dmac from the sample packet.		
max-export-pkt-size	Configure flow max export packet size .	integer	Minimum value: 512 Maximum value: 9216
timeout-general	Configure flow session general timeout .	integer	Minimum value: 60 Maximum value: 604800

Parameter	Description	Type	Size
timeout-icmp	Configure flow session ICMP timeout .	integer	Minimum value: 60 Maximum value: 604800
timeout-max	Configure flow session max timeout .	integer	Minimum value: 60 Maximum value: 604800
timeout-tcp	Configure flow session TCP timeout .	integer	Minimum value: 60 Maximum value: 604800
timeout-tcp-fin	Configure flow session TCP FIN timeout .	integer	Minimum value: 60 Maximum value: 604800
timeout-tcp-rst	Configure flow session TCP RST timeout .	integer	Minimum value: 60 Maximum value: 604800
timeout-udp	Configure flow session UDP timeout .	integer	Minimum value: 60 Maximum value: 604800

config aggregates

Parameter	Description	Type	Size
ip	IP address to group all matching traffic sessions to a flow.	ipv4-classnet	Not Specified

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
status	Enable/disable SNMP.	option	-
	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 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
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295

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
name	SNMP community name.	string	Maximum length: 35
status	Enable/disable this SNMP community.	option	-

Option	Description
disable	Disable SNMP community.
enable	Enable SNMP community.

Parameter	Description	Type	Size
query-v1-status	Enable/disable SNMP v1 queries.	option	-

Option	Description
disable	Disable SNMP v1 queries.
enable	Enable SNMP v1 queries.

query-v1-port	SNMP v1 query port .	integer	Minimum value: 0 Maximum value: 65535
query-v2c-status	Enable/disable SNMP v2c queries.	option	-

Option	Description
disable	Disable SNMP v2c queries.
enable	Enable SNMP v2c queries.

query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535
trap-v1-status	Enable/disable SNMP v1 traps.	option	-

Option	Description
disable	Disable SNMP v1 traps.
enable	Enable SNMP v1 traps.

trap-v1-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535
trap-v1-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-

Option	Description
disable	Disable SNMP v2c traps.
enable	Enable SNMP v2c traps.

Parameter	Description	Type	Size
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 0 Maximum value: 65535
events	SNMP notifications (traps) to send.	option	-

Option	Description
cpu-high	Send a trap when CPU usage too high.
mem-low	Send a trap when available memory is low.
log-full	Send a trap when log disk space becomes low.
intf-ip	Send a trap when an interface IP address is changed.
ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).

config hosts

Parameter	Description	Type	Size
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|sha]
      set auth-pwd {password}
      set priv-proto [aes|des]
      set priv-pwd {password}
   next
end
```

config switch-controller snmp-user

Parameter	Description	Type	Size
queries	Enable/disable SNMP queries for this user.	option	-

Option	Description
disable	Disable SNMP queries for this user.
enable	Enable SNMP queries for this user.

query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535
security-level	Security level for message authentication and encryption.	option	-

Option	Description
no-auth-no-priv	Message with no authentication and no privacy (encryption).
auth-no-priv	Message with authentication but no privacy (encryption).
auth-priv	Message with authentication and privacy (encryption).

auth-proto	Authentication protocol.	option	-

Option	Description
md5	HMAC-MD5-96 authentication protocol.
sha	HMAC-SHA-96 authentication protocol.

auth-pwd	Password for authentication protocol.	password	Not Specified
priv-proto	Privacy (encryption) protocol.	option	-

Option	Description
aes	CFB128-AES-128 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
mode	Configure traffic sniffer mode.	option	-

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

config target-mac

Parameter	Description	Type	Size
description	Description for the sniffer MAC.	string	Maximum length: 63

config target-ip

Parameter	Description	Type	Size
description	Description for the sniffer IP.	string	Maximum length: 63

config target-port

Parameter	Description	Type	Size
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
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-

Option	Description
enable	Enable logging by FortiSwitch device to a remote syslog server.
disable	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
severity	Severity of logs to be transferred to remote log server.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
csv	Enable/disable comma-separated value (CSV) strings.	option	-
	Option / **Description** *enable* — Enable comma-separated value (CSV) strings. *disable* — Disable comma-separated value (CSV) strings.		
facility	Facility to log to remote syslog server.	option	-
	Option / **Description** *kernel* — Kernel messages. *user* — Random user-level messages. *mail* — Mail system. *daemon* — System daemons. *auth* — Security/authorization messages. *syslog* — Messages generated internally by syslogd. *lpr* — Line printer subsystem. *news* — Network news subsystem. *uucp* — UUCP server messages. *cron* — Clock daemon. *authpriv* — Security/authorization messages (private). *ftp* — FTP daemon. *ntp* — NTP daemon.		

Parameter	Description	Type	Size

Option	Description
audit	Log audit.
alert	Log alert.
clock	Clock daemon.
local0	Reserved for local use.
local1	Reserved for local use.
local2	Reserved for local use.
local3	Reserved for local use.
local4	Reserved for local use.
local5	Reserved for local use.
local6	Reserved for local use.
local7	Reserved for local use.

system

This section includes syntax for the following commands:

- config system central-management on page 962
- config system info admin status on page 958
- config system auto-install on page 1040
- config system ha on page 872
- config system alias on page 957
- config system email-server on page 1027
- config system vdom-sflow on page 891
- config system proxy-arp on page 1033
- config system auto-script on page 957
- config system snmp community on page 921
- config system replacemsg admin on page 902
- config system lldp network-policy on page 1011
- config system gre-tunnel on page 977
- config system sms-server on page 842
- config system session-info full-stat on page 1052
- config system automation-trigger on page 1059
- config system session-ttl on page 932
- config system mobile-tunnel on page 980
- config system vdom-dns on page 893
- config system ips-urlfilter-dns6 on page 976
- config system api-user on page 849
- config system session6 on page 955
- config system vdom on page 740
- config system 3g-modem custom on page 953
- config system virtual-switch on page 834
- config system autoupdate schedule on page 930
- config system replacemsg ftp on page 898
- config system automation-stitch on page 1068
- config system source-ip status on page 1051
- config system session-helper-info list on page 1053
- config system settings on page 850
- config system session-info statistics on page 1052
- config system automation-destination on page 1067
- config system password-policy on page 837
- config system nd-proxy on page 1069
- config system speed-test-server on page 1010
- config system accprofile on page 774
- config system password-policy-guest-admin on page 840
- config system wccp on page 1046

- config system global on page 741
- config system dhcp6 server on page 944
- config system sdn-connector on page 968
- config system cluster-sync on page 1018
- config system csf on page 1057
- config system session-helper on page 1032
- config system automation-action on page 1062
- config system fortiguard on page 1021
- config system virtual-wan-link on page 995
- config system replacemsg sslvpn on page 903
- config system external-resource on page 974
- config system vxlan on page 984
- config system modem on page 946
- config system dns on page 886
- config system ipsec-aggregate on page 979
- config system ips-urlfilter-dns on page 975
- config system ip-conflict status on page 1053
- config system sflow on page 890
- config system fips-cc on page 1033
- config system vdom-link on page 788
- config system interface on page 793
- config system fortiguard-service on page 956
- config system replacemsg traffic-quota on page 906
- config system auto-update status on page 1052
- config system snmp sysinfo on page 920
- config system vdom-netflow on page 892
- config system ddns on page 888
- config system lte-modem on page 792
- config system status on page 954
- config system switch-interface on page 789
- config system mgmt-csum on page 956
- config system ntp on page 1042
- config system physical-switch on page 833
- config system replacemsg icap on page 907
- config system ptp on page 1045
- config system replacemsg http on page 896
- config system replacemsg-image on page 895
- config system probe-response on page 1036
- config system storage on page 883
- config system object-tagging on page 790
- config system arp-table on page 885
- config system arp on page 1027
- config system vdom-exception on page 1056
- config system ipv6-tunnel on page 973
- config system auto-update versions on page 1052

- config system fortisandbox on page 1055
- config system pppoe-interface on page 982
- config system alarm on page 1028
- config system virtual-wire-pair on page 986
- config system console on page 1041
- config system startup-error-log on page 1051
- config system geneve on page 985
- config system fsso-polling on page 871
- config system session-info expectation on page 1052
- config system dscp-based-priority on page 1035
- config system geoip-override on page 1054
- config system ipv6-neighbor-cache on page 886
- config system dhcp server on page 933
- config system info admin ssh on page 958
- config system management-tunnel on page 958
- config system replacemsg webproxy on page 897
- config system vdom-radius-server on page 1051
- config system nat64 on page 1049
- config system replacemsg device-detection-portal on page 904
- config system replacemsg spam on page 900
- config system performance top on page 954
- config system tos-based-priority on page 1034
- config system ipip-tunnel on page 979
- config system cmdb on page 955
- config system replacemsg-group on page 908
- config system performance status on page 954
- config system session on page 955
- config system fortimanager on page 960
- config system network-visibility on page 976
- config system vdom-property on page 993
- config system link-monitor on page 1037
- config system central-mgmt on page 957
- config system admin on page 842
- config system sso-admin on page 850
- config system netflow on page 892
- config system zone on page 966
- config system stp on page 836
- config system replacemsg nac-quar on page 905
- config system ha-monitor on page 882
- config system dedicated-mgmt on page 884
- config system checksum status on page 956
- config system replacemsg nntp on page 898
- config system mac-address-table on page 1031
- config system saml on page 1069
- config system replacemsg fortiguard-wf on page 899

- config system fortianalyzer-connectivity on page 956
- config system resource-limits on page 990
- config system session-info ttl on page 1053
- config system ha-nonsync-csum on page 956
- config system sit-tunnel on page 870
- config system performance firewall packet-distribution on page 955
- config system replacemsg mail on page 895
- config system snmp user on page 925
- config system fortiguard-log-service on page 956
- config system custom-language on page 842
- config system performance firewall statistics on page 955
- config system session-info list on page 1052
- config system npu on page 783
- config system geoip-country on page 967
- config system ftm-push on page 1053
- config system fm on page 961
- config system replacemsg utm on page 906
- config system dns-server on page 990
- config system dns-database on page 987
- config system replacemsg auth on page 902
- config system autoupdate tunneling on page 931
- config system autoupdate push-update on page 929
- config system replacemsg alertmail on page 901

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
short-name	VDOM short name.	string	Maximum length: 11

Parameter	Description	Type	Size
vcluster-id	Virtual cluster ID .	integer	Minimum value: 0 Maximum value: 4294967295
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295

config system global

Configure global attributes.

```
config system global
   Description: Configure global attributes.
   set language [english|french|...]
   set gui-ipv6 [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-fortisandbox-cloud [enable|disable]
   set gui-lines-per-page {integer}
   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 max-dlpstat-memory {integer}
   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 revision-image-auto-backup [enable|disable]
set revision-backup-on-logout [enable|disable]
set management-vdom {string}
set hostname {string}
set gui-allow-default-hostname [enable|disable]
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 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 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 strict-dirty-session-check [enable|disable]
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-timewait-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 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 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}
set dnsproxy-worker-count {integer}
set url-filter-count {integer}
set proxy-worker-count {integer}
set scanunit-count {integer}
set proxy-kxp-hardware-acceleration [disable|enable]
set proxy-cipher-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-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-policy [enable|disable]
    set log-uuid-address [enable|disable]
    set log-ssl-connection [enable|disable]
    set arp-max-entry {integer}
    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 device-identification-active-scan-delay {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 [green|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 fortitoken-cloud [enable|disable]
end
```

config system global

Parameter	Description	Type	Size
language	GUI display language.	option	-

Option	Description
english	English.
french	French.
spanish	Spanish.
portuguese	Portuguese.
japanese	Japanese.
trach	Traditional Chinese.
simch	Simplified Chinese.
korean	Korean.

gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Display the feature in GUI. *disable* 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	-
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.		
gui-custom-language	Enable/disable custom languages in GUI.	option	-
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.		
gui-wireless-opensecurity	Enable/disable wireless open security option on the GUI.	option	-
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.		
gui-display-hostname	Enable/disable displaying the FortiGate's hostname on the GUI login page.	option	-
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.		
gui-fortisandbox-cloud	Enable/disable displaying FortiSandbox Cloud on the GUI.	option	-
	Option **Description** *enable* Display the feature in GUI. *disable* Do not display the feature in GUI.		

Parameter	Description	Type	Size
gui-lines-per-page	Number of lines to display per page for web administration.	integer	Minimum value: 20 Maximum value: 1000
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-

Option	Description
tlsv1-1	TLS 1.1.
tlsv1-2	TLS 1.2.
tlsv1-3	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
admin-console-timeout	Console login timeout that overrides the admintimeout value. . 0 the default, disables this timeout.	integer	Minimum value: 15 Maximum value: 300
admin-concurrent	Enable/disable concurrent administrator logins. (Use policy-auth-concurrent for firewall authenticated users.)	option	-

Option	Description
enable	Enable admin concurrent login.
disable	Disable admin concurrent login.

admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 1 Maximum value: 10
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

Parameter	Description	Type	Size
refresh	Statistics refresh interval in GUI.	integer	Minimum value: 0 Maximum value: 4294967295
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295
daily-restart	Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.	option	-

Option	Description
enable	Enable daily reboot of the FortiGate.
disable	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
admin-login-max	Maximum number of administrators who can be logged in at the same time	integer	Minimum value: 1 Maximum value: 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
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds .	integer	Minimum value: 1 Maximum value: 300000

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable batch mode to execute in CMDB server.
disable	Disable batch mode to execute in CMDB server.

max-dlpstat-memory	Maximum DLP stat memory .	integer	Not Specified
multi-factor-authentication	Enforce all login methods to require an additional authentication factor .	option	-

Option	Description
optional	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).
mandatory	Enforce all login methods to require an additional authentication factor.

ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.
TLSv1-3	TLSv1.3.

autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-

Option	Description
enable	Enable automatic log partition check after ungraceful shutdown.
disable	Disable automatic log partition check after ungraceful shutdown.

dst	Enable/disable daylight saving time.	option	-

Option	Description
enable	Enable daylight saving time.
disable	Disable daylight saving time.

Parameter	Description	Type	Size
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	-

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
20	(GMT-3:00) Nuuk (Greenland)
75	(GMT-3:00) Uruguay
21	(GMT-2:00) Mid-Atlantic

Parameter	Description	Type	Size

Option	Description
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
43	(GMT+4:00) Baku
39	(GMT+3:00) St. Petersburg, Volgograd
44	(GMT+4:30) Kabul

Parameter	Description	Type	Size

Option	Description
46	(GMT+5:00) Islamabad, Karachi, Tashkent
47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi
51	(GMT+5:30) Sri Jayawardenepara
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
71	(GMT+12:00) Auckland, Wellington
72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.
00	(GMT+12:00) Eniwetok, Kwajalein

Parameter	Description	Type	Size
	Option **Description** *82* (GMT+12:45) Chatham Islands *73* (GMT+13:00) Nuku'alofa *86* (GMT+13:00) Samoa *76* (GMT+14:00) Kiritimati		
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-
	Option **Description** *tos* IP TOS. *dscp* DSCP (DiffServ) DS.		
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-
	Option **Description** *low* Low priority. *medium* Medium priority. *high* High priority.		
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-
	Option **Description** *disable* Disable anti-replay check. *loose* Loose anti-replay check. *strict* 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	-
	Option **Description** *enable* Enable sending of PMTU ICMP destination unreachable packet. *disable* Disable sending of PMTU ICMP destination unreachable packet.		

Parameter	Description	Type	Size
honor-df	Enable/disable honoring of Don't-Fragment (DF) flag.	option	-

Option	Description
enable	Enable honoring of Don't-Fragment flag.
disable	Disable honoring of Don't-Fragment flag.

Parameter	Description	Type	Size
pmtu-discovery	Enable/disable path MTU discovery.	option	-

Option	Description
enable	Enable path MTU discovery.
disable	Disable path MTU discovery.

Parameter	Description	Type	Size
revision-image-auto-backup	Enable/disable back-up of the latest configuration revision after the firmware is upgraded.	option	-

Option	Description
enable	Enable revision image backup automatically when upgrading image.
disable	Disable revision image backup automatically when upgrading image.

Parameter	Description	Type	Size
revision-backup-on-logout	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-

Option	Description
enable	Enable revision config backup automatically when logout.
disable	Disable revision config backup automatically when logout.

Parameter	Description	Type	Size
management-vdom	Management virtual domain name.	string	Maximum length: 31
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
gui-allow-default-hostname	Enable/disable the GUI warning about using a default hostname	option	-

Option	Description
enable	Stop the warning in the GUI.
disable	Show the warning in the GUI.

Parameter	Description	Type	Size
alias	Alias for your FortiGate unit.	string	Maximum length: 35
strong-crypto	Enable to use strong encryption and only allow strong ciphers (AES) and digest (SHA1) for HTTPS/SSH/TLS/SSL functions.	option	-

Option	Description
enable	Enable strong crypto for HTTPS/SSH/TLS/SSL.
disable	Disable strong crypto for HTTPS/SSH/TLS/SSL.

ssh-cbc-cipher	Enable/disable CBC cipher for SSH access.	option	-

Option	Description
enable	Enable CBC cipher for SSH access.
disable	Disable CBC cipher for SSH access.

ssh-hmac-md5	Enable/disable HMAC-MD5 for SSH access.	option	-

Option	Description
enable	Enable HMAC-MD5 for SSH access.
disable	Disable HMAC-MD5 for SSH access.

ssh-kex-sha1	Enable/disable SHA1 key exchange for SSH access.	option	-

Option	Description
enable	Enable SHA1 for SSH key exchanges.
disable	Disable SHA1 for SSH key exchanges.

ssh-mac-weak	Enable/disable HMAC-SHA1 and UMAC-64-ETM for SSH access.	option	-

Option	Description
enable	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.
disable	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.

ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable static key ciphers in SSL/TLS connections. *disable* — Disable static key ciphers in SSL/TLS connections.		
snat-route-change	Enable/disable the ability to change the static NAT route.	option	-
	Option / **Description** *enable* — Enable SNAT route change. *disable* — Disable SNAT route change.		
cli-audit-log	Enable/disable CLI audit log.	option	-
	Option / **Description** *enable* — Enable CLI audit log. *disable* — Disable CLI audit log.		
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-
	Option / **Description** *1024* — 1024 bits. *1536* — 1536 bits. *2048* — 2048 bits. *3072* — 3072 bits. *4096* — 4096 bits. *6144* — 6144 bits. *8192* — 8192 bits.		
fds-statistics	Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. This data is used to improve FortiGuard services and is not shared with external parties and is protected by Fortinet's privacy policy.	option	-
	Option / **Description** *enable* — Enable FortiGuard statistics. *disable* — Disable FortiGuard statistics.		

Parameter	Description	Type	Size
fds-statistics-period	FortiGuard statistics collection period in minutes. .	integer	Minimum value: 1 Maximum value: 1440
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-

Option	Description
enable	Enable TCP option.
disable	Disable TCP option.

Parameter	Description	Type	Size
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-

Option	Description
enable	Enable transmission of Link Layer Discovery Protocol (LLDP).
disable	Disable transmission of Link Layer Discovery Protocol (LLDP).

Parameter	Description	Type	Size
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-

Option	Description
enable	Enable reception of Link Layer Discovery Protocol (LLDP).
disable	Disable reception of Link Layer Discovery Protocol (LLDP).

Parameter	Description	Type	Size
proxy-auth-timeout	Authentication timeout in minutes for authenticated users .	integer	Minimum value: 1 Maximum value: 300
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	-

Option	Description
session	Proxy re-authentication timeout begins at the closure of the session.
traffic	Proxy re-authentication timeout begins after traffic has not been received.
absolute	Proxy re-authentication timeout begins when the user was first created.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable authenticated users lifetime control.
disable	Disable authenticated users lifetime control.

proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users .	integer	Minimum value: 5 Maximum value: 65535
sys-perf-log-interval	Time in minutes between updates of performance statistics logging. .	integer	Minimum value: 0 Maximum value: 15
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	-

Option	Description
loose	Check protocol header loosely.
strict	Check protocol header strictly.

vip-arp-range	Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.	option	-

Option	Description
unlimited	Send ARPs for all addresses in VIP range.
restricted	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	-

Option	Description
enable	Enable reset session-less TCP.
disable	Disable reset session-less TCP.

Parameter	Description	Type	Size
allow-traffic-redirect	Disable to allow traffic to be routed back on a different interface.	option	-

Option	Description
enable	Enable allow traffic redirect.
disable	Disable allow traffic redirect.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable strict dirty-session check.
disable	Disable strict dirty-session check.

Parameter	Description	Type	Size
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
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
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300
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
block-session-timer	Duration in seconds for blocked sessions .	integer	Minimum value: 1 Maximum value: 300

Parameter	Description	Type	Size
ip-src-port-range	IP source port range used for traffic originating from the FortiGate unit.	user	Not Specified
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-

Option	Description
enable	Enable pre-login banner.
disable	Disable pre-login banner.

Parameter	Description	Type	Size
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-

Option	Description
disable	Disable post-login banner.
enable	Enable post-login banner.

Parameter	Description	Type	Size
tftp	Enable/disable TFTP.	option	-

Option	Description
enable	Enable TFTP.
disable	Disable TFTP.

Parameter	Description	Type	Size
av-failopen	Set the action to take if the FortiGate is running low on memory or the proxy connection limit has been reached.	option	-

Option	Description
pass	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.
off	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.
one-shot	Bypass the antivirus system when memory is low.

Parameter	Description	Type	Size
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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable AV fail open session option. *disable* / Disable AV fail open session option.		
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme .	integer	Minimum value: 70 Maximum value: 97
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode .	integer	Minimum value: 70 Maximum value: 97
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode .	integer	Minimum value: 70 Maximum value: 97
cpu-use-threshold	Threshold at which CPU usage is reported. .	integer	Minimum value: 50 Maximum value: 99
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-
	Option / **Description** *strict* / Check RST range strictly. *disable* / Disable RST range check.		
vdom-mode *	Enable/disable support for split/multiple virtual domains (VDOMs).	option	-
	Option / **Description** *no-vdom* / Disable split/multiple VDOMs mode. *split-vdom* / Enable split VDOMs mode. *multi-vdom* / Enable multiple VDOMs mode.		
long-vdom-name *	Enable/disable long VDOM name support.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable long VDOM name support. *disable* / Disable long VDOM name support.		
admin-port	Administrative access port for HTTP. .	integer	Minimum value: 1 Maximum value: 65535
admin-sport	Administrative access port for HTTPS. .	integer	Minimum value: 1 Maximum value: 65535
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-
	Option / **Description** *enable* / Enable redirecting HTTP administration access to HTTPS. *disable* / 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
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-
	Option / **Description** *enable* / Enable password authentication for SSH admin access. *disable* / Disable password authentication for SSH admin access.		
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running.	option	-
	Option / **Description** *enable* / Enable local admin authentication restriction. *disable* / Disable local admin authentication restriction.		

Parameter	Description	Type	Size
admin-ssh-port	Administrative access port for SSH. .	integer	Minimum value: 1 Maximum value: 65535
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
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-

Option	Description
enable	Enable SSH v1 compatibility.
disable	Disable SSH v1 compatibility.

admin-telnet	Enable/disable TELNET service.	option	-

Option	Description
enable	Enable TELNET service.
disable	Disable TELNET service.

admin-telnet-port	Administrative access port for TELNET. .	integer	Minimum value: 1 Maximum value: 65535
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	-

Option	Description
enable	Enable login for special user (maintainer).
disable	Disable login for special user (maintainer).

admin-reset-button *	press the reset button can reset to factory default	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — press the reset button can reset to factory default *disable* — 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
user-server-cert	Certificate to use for https user authentication.	string	Maximum length: 35
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	-
	Option / **Description** *enable* — Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access. *disable* — Admin users can login by providing a valid certificate or password.		
wifi-certificate	Certificate to use for WiFi authentication.	string	Maximum length: 35
wifi-ca-certificate	CA certificate that verifies the WiFi certificate.	string	Maximum length: 79
auth-http-port	User authentication HTTP port. .	integer	Minimum value: 1 Maximum value: 65535
auth-https-port	User authentication HTTPS port. .	integer	Minimum value: 1 Maximum value: 65535
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-
	Option / **Description** *enable* — Enable use of keep alive to extend authentication. *disable* — Disable use of keep alive to extend authentication.		

Parameter	Description	Type	Size
policy-auth-concurrent	Number of concurrent firewall use logins from the same user .	integer	Minimum value: 0 Maximum value: 100
auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-

Option	Description
block-new	Block new user authentication attempts.
logout-inactive	Logout the most inactive user authenticated sessions.

Parameter	Description	Type	Size
auth-cert	Server certificate that the FortiGate uses for HTTPS firewall authentication connections.	string	Maximum length: 35
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-

Option	Description
enable	Enable require client certificate for GUI login.
disable	Disable require client certificate for GUI login.

Parameter	Description	Type	Size
fortiservice-port	FortiService port . Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535
cfg-save	Configuration file save mode for CLI changes.	option	-

Option	Description
automatic	Automatically save config.
manual	Manually save config.
revert	Manually save config and revert the config when timeout.

Parameter	Description	Type	Size
cfg-revert-timeout	Time-out for reverting to the last saved configuration.	integer	Minimum value: 10 Maximum value: 4294967295
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable reboot of system upon restoring configuration. *disable* 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	-
	Option **Description** *enable* Enable allow system configuration download by SCP. *disable* Disable allow system configuration download by SCP.		
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-
	Option **Description** *enable* Enable submission of Security Rating results to FortiGuard. *disable* Disable submission of Security Rating results to FortiGuard.		
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-
	Option **Description** *enable* Enable scheduled runs of Security Rating. *disable* Disable scheduled runs of Security Rating.		
wireless-controller	Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.	option	-
	Option **Description** *enable* Enable wireless controller. *disable* Disable wireless controller.		
wireless-controller-port	Port used for the control channel in wireless controller mode .	integer	Minimum value: 1024 Maximum value: 49150

Parameter	Description	Type	Size
fortiextender-data-port	FortiExtender data port .	integer	Minimum value: 1024 Maximum value: 49150
fortiextender	Enable/disable FortiExtender.	option	-

Option	Description
disable	Disable FortiExtender controller.
enable	Enable FortiExtender controller.

fortiextender-vlan-mode	Enable/disable FortiExtender VLAN mode.	option	-

Option	Description
enable	Enable FortiExtender VLAN mode.
disable	Disable FortiExtender VLAN mode.

switch-controller	Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself.	option	-

Option	Description
disable	Disable switch controller feature.
enable	Enable switch controller feature.

switch-controller-reserved-network	Enable reserved network subnet for controlled switches. This is available when the switch controller is enabled.	ipv4-classnet	Not Specified
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: The number of logical CPUs **
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1 **
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 4 **

Parameter	Description	Type	Size
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 **
proxy-kxp-hardware-acceleration	Enable/disable using the content processor to accelerate KXP traffic.	option	-

Option	Description
disable	Disable using the content processor to accelerate KXP traffic.
enable	Enable using the content processor to accelerate KXP traffic.

proxy-cipher-hardware-acceleration	Enable/disable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.	option	-

Option	Description
disable	Disable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.
enable	Enable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.

fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-

Option	Description
advisory	Retrieve FortiGuard advisories, report and news alerts.
latest-threat	Retrieve latest FortiGuard threats alerts.
latest-virus	Retrieve latest FortiGuard virus alerts.
latest-attack	Retrieve latest FortiGuard attack alerts.
new-antivirus-db	Retrieve FortiGuard AV database release alerts.
new-attack-db	Retrieve FortiGuard IPS database release alerts.

ipsec-hmac-offload	Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.	option	-

Option	Description
enable	Enable offload IPsec HMAC processing to hardware if possible.
disable	Disable offload IPsec HMAC processing to hardware.

Parameter	Description	Type	Size
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2
ipv6-allow-anycast-probe	Enable/disable IPv6 address probe through Anycast.	option	-

Option	Description
enable	Enable probing of IPv6 address space through Anycast
disable	Disable probing of IPv6 address space through Anycast

Parameter	Description	Type	Size
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-

Option	Description
enable	Enable CA attribute in CSR.
disable	Disable CA attribute in CSR.

Parameter	Description	Type	Size
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-

Option	Description
enable	Enable WiMax 4G.
disable	Disable WiMax 4G.

Parameter	Description	Type	Size
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647
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.	integer	Minimum value: 0 Maximum value: 4 **
sslvpn-kxp-hardware-acceleration *	Enable/disable SSL VPN KXP hardware acceleration.	option	-

Option	Description
enable	Enable KXP SSL-VPN hardware acceleration.
disable	Disable KXP SSL-VPN hardware acceleration.

Parameter	Description	Type	Size
sslvpn-cipher-hardware-acceleration *	Enable/disable SSL VPN hardware acceleration.	option	-

Option	Description
enable	Enable SSL-VPN cipher hardware acceleration.
disable	Disable SSL-VPN cipher hardware acceleration.

sslvpn-plugin-version-check	Enable/disable checking browser's plugin version by SSL VPN.	option	-

Option	Description
enable	Enable SSL-VPN automatic checking of browser plug-in version.
disable	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
two-factor-email-expiry	Email-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300
two-factor-sms-expiry	SMS-based two-factor authentication session timeout .	integer	Minimum value: 30 Maximum value: 300
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout .	integer	Minimum value: 10 Maximum value: 3600
two-factor-ftm-expiry	FortiToken Mobile session timeout .	integer	Minimum value: 1 Maximum value: 168
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 **

Parameter	Description	Type	Size
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 4 **
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-

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
login-timestamp	Enable/disable login time recording.	option	-

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
special-file-23-support	Enable/disable IPS detection of HIBUN format files when using Data Leak Protection.	option	-

Option	Description
disable	Disable using IPS detection of HIBUN format files when using Data Leak Protection.
enable	Enable using IPS detection of HIBUN format files when using Data Leak Protection.

log-uuid-policy	Enable/disable insertion of policy UUIDs to traffic logs.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable insertion of policy UUID to traffic logs. *disable* Disable insertion of policy UUID to traffic logs.		
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-
	Option **Description** *enable* Enable insertion of address UUID to traffic logs. *disable* Disable insertion of address UUID to traffic logs.		
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-
	Option **Description** *enable* Enable logging of SSL connection events. *disable* Disable logging of SSL connection events.		
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
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
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647
max-route-cache-size	Maximum number of IP route cache entries .	integer	Minimum value: 0 Maximum value: 2147483647

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable ASIC offload for IPsec VPN.
disable	Disable ASIC offload for IPsec VPN.

Parameter	Description	Type	Size
ipsec-soft-dec-async	Enable/disable software decryption asynchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-

Option	Description
enable	Enable software decryption asynchronization for IPsec VPN.
disable	Disable software decryption asynchronization for IPsec VPN.

Parameter	Description	Type	Size
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
device-identification-active-scan-delay	Number of seconds to passively scan a device before performing an active scan. .	integer	Minimum value: 20 Maximum value: 3600
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 passpharse.	option	-

Option	Description
disable	Disable private data encryption using an AES 128-bit key.
enable	Enable private data encryption using an AES 128-bit key.

Parameter	Description	Type	Size
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable automatic authorization of dedicated Fortinet extension device globally. *disable* — Disable automatic authorization of dedicated Fortinet extension device globally.		
gui-theme	Color scheme for the administration GUI.	option	-
	Option / **Description** *green* — Green theme. *neutrino* — Neutrino theme. *blue* — Light blue theme. *melongene* — Melongene theme (eggplant color). *mariner* — Mariner theme (dark blue color).		
gui-date-format	Default date format used throughout GUI.	option	-
	Option / **Description** *yyyy/MM/dd* — Year/Month/Day. *dd/MM/yyyy* — Day/Month/Year. *MM/dd/yyyy* — Month/Day/Year. *yyyy-MM-dd* — Year-Month-Day. *dd-MM-yyyy* — Day-Month-Year. *MM-dd-yyyy* — Month-Day-Year.		
gui-date-time-source	Source from which the FortiGate GUI uses to display date and time entries.	option	-
	Option / **Description** *system* — Use this FortiGate unit's configured timezone. *browser* — Use the web browser's timezone.		
igmp-state-limit	Maximum number of IGMP memberships .	integer	Minimum value: 96 Maximum value: 128000
legacy-poe-device-support *	Enable/disable legacy POE device support.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable legacy POE device support. *disable* — Disable legacy POE device support.		
cloud-communication	Enable/disable all cloud communication.	option	-
	Option / **Description** *enable* — Allow cloud communication. *disable* — Disable all cloud communication. When set to *disable*, cloud-related settings (for example, config system autoupdate tunneling on page 931 status) will be disabled. When a user issues the command to change one of these settings, it will fail with the message *cloud communication is disabled in 'system.global'*.		
fec-port	Local UDP port for Forward Error Correction .	integer	Minimum value: 49152 Maximum value: 65535
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-
	Option / **Description** *enable* — Enable FortiToken Cloud service. *disable* — Disable FortiToken Cloud service.		

* 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|...]
      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 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}
   next
end
```

config system accprofile

Parameter	Description	Type	Size
scope	Scope of admin access: global or specific VDOM(s).	option	-

Parameter	Description	Type	Size
	Option **Description** *vdom* VDOM access. *global* Global access.		
comments	Comment.	var-string	Maximum length: 255
secfabgrp	Security Fabric.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		
ftviewgrp	FortiView.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		
authgrp	Administrator access to Users and Devices.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		
sysgrp	System Configuration.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access. *custom* Customized access.		
netgrp	Network Configuration.	option	-

Parameter	Description	Type	Size
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.		
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.		
fwgrp	Administrator access to the Firewall configuration.	option	-
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access. *custom* — Customized access.		
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.		
utmgrp	Administrator access to Security Profiles.	option	-
	Option / **Description** *none* — No access. *read* — Read access.		

Parameter	Description	Type	Size
	Option / **Description** *read-write* — Read/write access. *custom* — Customized access.		
wifi	Administrator access to the WiFi controller and Switch controller.	option	-
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.		
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-
	Option / **Description** *enable* — Enable overriding the global administrator idle timeout. *disable* — Disable overriding the global administrator idle timeout.		
admintimeout	Administrator timeout for this access profile .	integer	Minimum value: 1 Maximum value: 480

config netgrp-permission

Parameter	Description	Type	Size
cfg	Network Configuration.	option	-
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.		
packet-capture	Packet Capture Configuration.	option	-
	Option / **Description** *none* — No access. *read* — Read access. *read-write* — Read/write access.		

Parameter	Description	Type	Size
route-cfg	Router Configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

config sysgrp-permission

Parameter	Description	Type	Size
admin	Administrator Users.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
upd	FortiGuard Updates.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
cfg	System Configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
mnt	Maintenance.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

config fwgrp-permission

Parameter	Description	Type	Size
policy	Policy Configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
address	Address Configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
service	Service Configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
schedule	Schedule Configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

config loggrp-permission

Parameter	Description	Type	Size
config	Log & Report configuration.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
data-access	Log & Report Data Access.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
report-access	Log & Report Report Access.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
threat-weight	Log & Report Threat Weight.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

config utmgrp-permission

Parameter	Description	Type	Size
antivirus	Antivirus profiles and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
ips	IPS profiles and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
webfilter	Web Filter profiles and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
emailfilter	AntiSpam filter and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
data-loss-prevention	DLP profiles and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
application-control	Application Control profiles and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
icap	ICAP profiles and settings.	option	-

Option	Description
none	No access.
read	Read access.
read-write	Read/write access.

Parameter	Description	Type	Size
voip	VoIP profiles and settings.	option	-

Parameter	Description	Type	Size
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		
waf	Web Application Firewall profiles and settings.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		
dnsfilter	DNS Filter profiles and settings.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		
endpoint-control	FortiClient Profiles.	option	-
	Option **Description** *none* No access. *read* Read access. *read-write* Read/write access.		

config system npu

This command is available for reference model(s) FortiGate 80E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61E. 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
iph-rsvd-re-cksum *	Enable/disable IP checksum re-calculation for packets with iph.reserved bit set.	option	-

Option	Description
enable	Enable IP checksum re-calculation for packets with iph.reserved bit set.
disable	Disable IP checksum re-calculation for packets with iph.reserved bit set.

Parameter	Description	Type	Size
per-session-accounting *	Enable/disable per-session accounting.	option	-

Option	Description
disable	Disable per-session accounting.
traffic-log-only	Per-session accounting only for sessions with traffic logging enabled in firewall policy.
enable	Per-session accounting for all sessions.

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size
ipv4-ver-err	Invalid IPv4 header version anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid header version.
trap-to-host	Forward IPv4 invalid header version to main CPU for processing.

Parameter	Description	Type	Size
ipv4-ihl-err	Invalid IPv4 header length anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid header length.
trap-to-host	Forward IPv4 invalid header length to main CPU for processing.

Parameter	Description	Type	Size
ipv4-len-err	Invalid IPv4 packet length anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid packet length.
trap-to-host	Forward IPv4 invalid packet length to main CPU for processing.

Parameter	Description	Type	Size
ipv4-ttlzero-err	Invalid IPv4 TTL field zero anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid TTL field zero.
trap-to-host	Forward IPv4 invalid TTL field zero to main CPU for processing.

Parameter	Description	Type	Size
ipv4-csum-err	Invalid IPv4 packet checksum anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid L3 checksum.
trap-to-host	Forward IPv4 invalid L3 checksum to main CPU for processing.

Parameter	Description	Type	Size
ipv4-opt-err	Invalid IPv4 option parsing anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid option parsing.
trap-to-host	Forward IPv4 invalid option parsing to main CPU for processing.

Parameter	Description	Type	Size
tcp-hlen-err	Invalid IPv4 TCP header length anomalies.	option	-

Parameter	Description	Type	Size
	Option **Description** *drop* Drop IPv4 invalid TCP packet header length. *trap-to-host* Forward IPv4 invalid TCP packet header length to main CPU for processing.		
tcp-plen-err	Invalid IPv4 TCP packet length anomalies.	option	-
	Option **Description** *drop* Drop IPv4 invalid TCP packet length. *trap-to-host* Forward IPv4 invalid TCP packet length to main CPU for processing.		
tcp-csum-err	Invalid IPv4 TCP packet checksum anomalies.	option	-
	Option **Description** *drop* Drop IPv4 invalid TCP packet checksum. *trap-to-host* Forward IPv4 invalid TCP packet checksum to main CPU for processing.		
udp-plen-err	Invalid IPv4 UDP packet minimum length anomalies.	option	-
	Option **Description** *drop* Drop IPv4 invalid UDP packet minimum length. *trap-to-host* Forward IPv4 invalid UDP packet minimum length to main CPU for processing.		
udp-hlen-err	Invalid IPv4 UDP packet header length anomalies.	option	-
	Option **Description** *drop* Drop IPv4 invalid UDP header length. *trap-to-host* Forward IPv4 invalid UDP header length to main CPU for processing.		
udp-csum-err	Invalid IPv4 UDP packet checksum anomalies.	option	-
	Option **Description** *drop* Drop IPv4 invalid UDP packet checksum. *trap-to-host* Forward IPv4 invalid UDP packet checksum to main CPU for processing.		
udp-len-err	Invalid IPv4 UDP packet length anomalies.	option	-
	Option **Description** *drop* Drop IPv4 invalid UDP packet length. *trap-to-host* Forward IPv4 invalid UDP packet length to main CPU for processing.		

Parameter	Description	Type	Size
udplite-cover-err	Invalid IPv4 UDP-Lite packet coverage anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid UDP-Lite packet coverage.
trap-to-host	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.

udplite-csum-err	Invalid IPv4 UDP-Lite packet checksum anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid UDP-Lite packet checksum.
trap-to-host	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.

icmp-minlen-err	Invalid IPv4 ICMP short packet anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid ICMP short packet.
trap-to-host	Forward IPv4 invalid ICMP short packet to main CPU for processing.

icmp-csum-err	Invalid IPv4 ICMP packet checksum anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid ICMP checksum.
trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.

esp-minlen-err	Invalid IPv4 ESP short packet anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid ESP short packet.
trap-to-host	Forward IPv4 invalid ESP short packet to main CPU for processing.

unknproto-minlen-err	Invalid IPv4 L4 unknown protocol short packet anomalies.	option	-

Option	Description
drop	Drop IPv4 invalid L4 unknown protocol short packet.
trap-to-host	Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.

Parameter	Description	Type	Size
ipv6-ver-err	Invalid IPv6 packet version anomalies.	option	-

Option	Description
drop	Drop IPv6 with invalid packet version.
trap-to-host	Forward IPv6 with invalid packet version to FortiOS.

Parameter	Description	Type	Size
ipv6-ihl-err	Invalid IPv6 packet length anomalies.	option	-

Option	Description
drop	Drop IPv6 with invalid packet length.
trap-to-host	Forward IPv6 with invalid packet length to FortiOS.

Parameter	Description	Type	Size
ipv6-plen-zero	Invalid IPv6 packet payload length zero anomalies.	option	-

Option	Description
drop	Drop IPv6 with invalid packet payload length zero.
trap-to-host	Forward IPv6 with invalid packet payload length zero to FortiOS.

Parameter	Description	Type	Size
ipv6-exthdr-order-err	Invalid IPv6 packet extension header ordering anomalies.	option	-

Option	Description
drop	Drop IPv6 with invalid packet extension header ordering.
trap-to-host	Forward IPv6 with invalid packet extension header ordering to FortiOS.

Parameter	Description	Type	Size
ipv6-exthdr-len-err	Invalid IPv6 packet chain extension header total length anomalies.	option	-

Option	Description
drop	Drop IPv6 with invalid packet chain extension header total length.
trap-to-host	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
vcluster	Virtual cluster.	option	-

Option	Description
vcluster1	Virtual cluster 1.
vcluster2	Virtual cluster 2.

Parameter	Description	Type	Size
type	VDOM link type: PPP or Ethernet.	option	-

Option	Description
ppp	PPP VDOM link.
ethernet	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 span [disable|enable]
      set span-direction [rx|tx|...]
   next
end
```

config system switch-interface

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
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	-

Option	Description
switch	Switch for normal switch functionality (available in NAT mode only).
hub	Hub to duplicate packets to all member ports.

Parameter	Description	Type	Size
intra-switch-policy	Allow any traffic between switch interfaces or require firewall policies to allow traffic between switch interfaces.	option	-

Option	Description
implicit	Traffic between switch members is implicitly allowed.
explicit	Traffic between switch members must match firewall policies.

Parameter	Description	Type	Size
span	Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span destination port.	option	-

Option	Description
disable	Disable port spanning.
enable	Enable port spanning.

Parameter	Description	Type	Size
span-direction	The direction in which the SPAN port operates, either: rx, tx, or both.	option	-

Option	Description
rx	Copies only received packets from source SPAN ports to the destination SPAN port.
tx	Copies only transmitted packets from source SPAN ports to the destination SPAN port.
both	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.

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
address	Address.	option	-

Option	Description
disable	Disable.
mandatory	Mandatory.
optional	Optional.

Parameter	Description	Type	Size
device	Device.	option	-

Option	Description
disable	Disable.
mandatory	Mandatory.
optional	Optional.

Parameter	Description	Type	Size
interface	Interface.	option	-

Option	Description
disable	Disable.
mandatory	Mandatory.
optional	Optional.

Parameter	Description	Type	Size
multiple	Allow multiple tag selection.	option	-

Option	Description
enable	Enable multi-tagging.
disable	Disable multi-tagging.

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
tags <name>	Tags. Tag name.	string	Maximum length: 79

config system lte-modem

This command is available for reference model(s) FortiGate 80E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61E. 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
status	Enable/disable USB LTE/WIMAX device.	option	-
	Option / **Description** *enable* / Enable USB LTE/WIMA device. *disable* / 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	-

Parameter	Description	Type	Size
	Option / **Description** *none* — Username and password not required. *pap* — Use PAP authentication. *chap* — Use CHAP authentication.		
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
mode	Modem operation mode.	option	-
	Option / **Description** *standalone* — Standalone modem operation mode. *redundant* — 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
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 mode [static|dhcp|...]
      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-type [regular|ipsec]
set dhcp-relay-agent-option [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 vlanid {integer}
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 {string}
set security-external-logout {string}
set replacemsg-override-group {string}
set security-redirect-url {string}
set security-exempt-list {string}
set security-groups <name1>, <name2>, ...
set stp [disable|enable]
set stp-ha-slave [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 broadcast-forticlient-discovery [enable|disable]
set estimated-upstream-bandwidth {integer}
set estimated-downstream-bandwidth {integer}
set vrrp-virtual-mac [enable|disable]
config vrrp
   Description: VRRP configuration.
   edit <vrid>
      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-stacking [enable|disable]
set fortilink-neighbor-detect [lldp|fortilink]
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-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]
set switch-controller-arp-inspection [enable|disable]
set switch-controller-learning-limit {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 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 ip6-reachable-time {integer}
set ip6-retrans-time {integer}
set ip6-default-life {integer}
set ip6-hop-limit {integer}
set autoconf [enable|disable]
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 vrrp-virtual-mac6 [enable|disable]
set vrip6_link_local {ipv6-address}
config vrrp6
   Description: IPv6 VRRP configuration.
   edit <vrid>
      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
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295
fortilink	Enable FortiLink to dedicate this interface to manage other Fortinet devices.	option	-

Option	Description
enable	Enable FortiLink to dedicated interface for managing FortiSwitch devices.
disable	Disable FortiLink to dedicated interface for managing FortiSwitch devices.

mode	Addressing mode (static, DHCP, PPPoE).	option	-

Option	Description
static	Static setting.
dhcp	External DHCP client mode.
pppoe	External PPPoE mode.

Parameter	Description	Type	Size
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	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	-

Option	Description
disable	None.
enable	DHCP relay agent.

dhcp-relay-ip	DHCP relay IP address.	user	Not Specified
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-

Option	Description
regular	Regular DHCP relay.
ipsec	DHCP relay for IPsec.

dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-

Option	Description
enable	Enable DHCP relay agent option.
disable	Disable DHCP relay agent option.

Parameter	Description	Type	Size
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified
allowaccess	Permitted types of management access to this interface.	option	-

Option	Description
ping	PING access.
https	HTTPS access.
ssh	SSH access.
snmp	SNMP access.
http	HTTP access.
telnet	TELNET access.
fgfm	FortiManager access.
radius-acct	RADIUS accounting access.
probe-response	Probe access.
fabric	Security Fabric access.
ftm	FTM access.

gwdetect	Enable/disable detect gateway alive for first.	option	-

Option	Description
enable	Enable detect gateway alive for first.
disable	Disable detect gateway alive for first.

ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255
detectserver	Gateway's ping server for this IP.	user	Not Specified
detectprotocol	Protocols used to detect the server.	option	-

Option	Description
ping	PING.
tcp-echo	TCP echo.

Parameter	Description	Type	Size
	Option **Description** *udp-echo* UDP echo.		
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50
fail-detect	Enable/disable fail detection features for this interface.	option	-
	Option **Description** *enable* Enable interface failed option status. *disable* Disable interface failed option status.		
fail-detect-option	Options for detecting that this interface has failed.	option	-
	Option **Description** *detectserver* Use a ping server to determine if the interface has failed. *link-down* 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	-
	Option **Description** *link-failed-signal* Link-failed-signal. *link-down* Link-down.		
fail-action-on-extender	Action on extender when interface fail .	option	-
	Option **Description** *soft-restart* Soft-restart-on-extender. *hard-restart* Hard-restart-on-extender. *reboot* 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

Parameter	Description	Type	Size
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
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-

Option	Description
enable	Enable IP address negotiating for unnumbered.
disable	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
detected-peer-mtu	MTU of detected peer .	integer	Minimum value: 0 Maximum value: 4294967295
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
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295
service-name	PPPoE service name.	string	Maximum length: 63

Parameter	Description	Type	Size
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
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-

Option	Description
enable	Enable default gateway.
disable	Disable default gateway.

Parameter	Description	Type	Size
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-

Option	Description
enable	Use DNS acquired by DHCP or PPPoE.
disable	No not use DNS acquired by DHCP or PPPoE.

Parameter	Description	Type	Size
auth-type	PPP authentication type to use.	option	-

Option	Description
auto	Automatically choose authentication.
pap	PAP authentication.
chap	CHAP authentication.
mschapv1	MS-CHAPv1 authentication.
mschapv2	MS-CHAPv2 authentication.

Parameter	Description	Type	Size
pptp-client	Enable/disable PPTP client.	option	-

Option	Description
enable	Enable PPTP client.
disable	Disable PPTP client.

Parameter	Description	Type	Size
pptp-user	PPTP user name.	string	Maximum length: 64
pptp-password	PPTP password.	password	Not Specified
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified
pptp-auth-type	PPTP authentication type.	option	-

Option	Description
auto	Automatically choose authentication.
pap	PAP authentication.
chap	CHAP authentication.
mschapv1	MS-CHAPv1 authentication.
mschapv2	MS-CHAPv2 authentication.

pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535
arpforward	Enable/disable ARP forwarding.	option	-

Option	Description
enable	Enable ARP forwarding.
disable	Disable ARP forwarding.

ndiscforward	Enable/disable NDISC forwarding.	option	-

Option	Description
enable	Enable NDISC forwarding.
disable	Disable NDISC forwarding.

broadcast-forward	Enable/disable broadcast forwarding.	option	-

Option	Description
enable	Enable broadcast forwarding.
disable	Disable broadcast forwarding.

bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-

Parameter	Description	Type	Size
	Option / **Description** *global* — BFD behavior of this interface will be based on global configuration. *enable* — Enable BFD on this interface and ignore global configuration. *disable* — 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
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000
l2forward	Enable/disable l2 forwarding.	option	-
	Option / **Description** *enable* — Enable L2 forwarding. *disable* — Disable L2 forwarding.		
icmp-send-redirect	Enable/disable ICMP send redirect.	option	-
	Option / **Description** *enable* — Enable ICMP send redirect. *disable* — Disable ICMP send redirect.		
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-
	Option / **Description** *enable* — Enable ICMP accept redirect. *disable* — Disable ICMP accept redirect.		
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable traffic forwarding. *disable* — Disable traffic forwarding.		
stpforward	Enable/disable STP forwarding.	option	-
	Option / **Description** *enable* — Enable STP forwarding. *disable* — Disable STP forwarding.		
stpforward-mode	Configure STP forwarding mode.	option	-
	Option / **Description** *rpl-all-ext-id* — Replace all extension IDs (root, bridge). *rpl-bridge-ext-id* — Replace the bridge extension ID only. *rpl-nothing* — Replace nothing.		
ips-sniffer-mode	Enable/disable the use of this interface as a one-armed sniffer.	option	-
	Option / **Description** *enable* — Enable IPS sniffer mode. *disable* — Disable IPS sniffer mode.		
ident-accept	Enable/disable authentication for this interface.	option	-
	Option / **Description** *enable* — Enable determining a user's identity from packet identification. *disable* — Disable determining a user's identity from packet identification.		
ipmac	Enable/disable IP/MAC binding.	option	-
	Option / **Description** *enable* — Enable IP/MAC binding. *disable* — Disable IP/MAC binding.		
subst	Enable to always send packets from this interface to a destination MAC address.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Send packets from this interface. *disable* / 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
poe *	Enable/disable PoE status.	option	-
	Option / **Description** *enable* / Enable PoE status. *disable* / Disable PoE status.		
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-
	Option / **Description** *auto* / Automatically adjust speed. *10full* / 10M full-duplex. *10half* / 10M half-duplex. *100full* / 100M full-duplex. *100half* / 100M half-duplex. *1000full* / 1000M full-duplex. *1000half* / 1000M half-duplex. *1000auto* / 1000M auto adjust.		
status	Bring the interface up or shut the interface down.	option	-
	Option / **Description** *up* / Bring the interface up. *down* / Shut the interface down.		
netbios-forward	Enable/disable NETBIOS forwarding.	option	-
	Option / **Description** *disable* / Disable NETBIOS forwarding.		

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable NETBIOS forwarding.		
wins-ip	WINS server IP.	ipv4-address	Not Specified
type	Interface type.	option	-
	Option / **Description** *physical* / Physical interface. *vlan* / VLAN interface. *aggregate* / Aggregate interface. *redundant* / Redundant interface. *tunnel* / Tunnel interface. *vdom-link* / VDOM link interface. *loopback* / Loopback interface. *switch* / Software switch interface. *hard-switch* / Hardware switch interface. *vap-switch* / VAP interface. *wl-mesh* / WLAN mesh interface. *fext-wan* / FortiExtender interface. *vxlan* / VXLAN interface. *geneve* / GENEVE interface. *hdlc* / T1/E1 interface. *switch-vlan* / Switch VLAN interface. *emac-vlan* / EMAC VLAN interface.		
dedicated-to	Configure interface for single purpose.	option	-
	Option / **Description** *none* / Interface not dedicated for any purpose. *management* / 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
trust-ip-2	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified

Parameter	Description	Type	Size
trust-ip-3	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified
trust-ip6-1	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified
trust-ip6-2	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified
trust-ip6-3	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified
mtu-override	Enable to set a custom MTU for this interface.	option	-

Option	Description
enable	Override default MTU.
disable	Use default MTU (1500).

mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-

Option	Description
enable	Enable WCCP protocol on this interface.
disable	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	-

Option	Description
disable	Disable NetFlow protocol on this interface.
tx	Monitor transmitted traffic on this interface.
rx	Monitor received traffic on this interface.
both	Monitor transmitted/received traffic on this interface.

sflow-sampler	Enable/disable sFlow on this interface.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable sFlow protocol on this interface. *disable* Disable sFlow protocol on this interface.		
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-
	Option **Description** *enable* Enable drop of overlapped fragment packets. *disable* Disable drop of overlapped fragment packets.		
drop-fragment	Enable/disable drop fragment packets.	option	-
	Option **Description** *enable* Enable/disable drop fragment packets. *disable* Do not drop fragment packets.		
src-check	Enable/disable source IP check.	option	-
	Option **Description** *enable* Enable source IP check. *disable* Disable source IP check.		
sample-rate	sFlow sample rate .	integer	Minimum value: 10 Maximum value: 99999
polling-interval	sFlow polling interval .	integer	Minimum value: 1 Maximum value: 255
sample-direction	Data that NetFlow collects (rx, tx, or both).	option	-
	Option **Description** *tx* Monitor transmitted traffic on this interface. *rx* Monitor received traffic on this interface. *both* Monitor transmitted/received traffic on this interface.		
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable explicit Web proxy on this interface. *disable* — Disable explicit Web proxy on this interface.		
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-
	Option / **Description** *enable* — Enable explicit FTP proxy on this interface. *disable* — Disable explicit FTP proxy on this interface.		
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-
	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
inbandwidth	Bandwidth limit for incoming traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000
outbandwidth	Bandwidth limit for outgoing traffic .	integer	Minimum value: 0 Maximum value: 16776000
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

Parameter	Description	Type	Size
spillover-threshold	Egress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000
ingress-spillover-threshold	Ingress Spillover threshold .	integer	Minimum value: 0 Maximum value: 16776000
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255
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	-

Option	Description
enable	Enable identifying the interface as an external interface.
disable	Disable identifying the interface as an external interface.

vlanid	VLAN ID .	integer	Minimum value: 1 Maximum value: 4094
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 Maximum value: 2147483647
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified
member `<interface-name>`	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79
lacp-mode	LACP mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *static* — Use static aggregation, do not send and ignore any LACP messages. *passive* — Passively use LACP to negotiate 802.3ad aggregation. *active* — Actively use LACP to negotiate 802.3ad aggregation.		
lacp-ha-slave	LACP HA slave.	option	-
	Option / **Description** *enable* — Allow HA slave to send/receive LACP messages. *disable* — Block HA slave from sending/receiving LACP messages.		
lacp-speed	How often the interface sends LACP messages.	option	-
	Option / **Description** *slow* — Send LACP message every 30 seconds. *fast* — Send LACP message every second.		
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32
min-links-down	Action to take when less than the configured minimum number of links are active.	option	-
	Option / **Description** *operational* — Set the aggregate operationally down. *administrative* — Set the aggregate administratively down.		
algorithm	Frame distribution algorithm.	option	-
	Option / **Description** *L2* — Use layer 2 address for distribution. *L3* — Use layer 3 address for distribution. *L4* — Use layer 4 information for distribution.		
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000

Parameter	Description	Type	Size
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-

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
vindex	Switch control interface VLAN ID.	integer	Minimum value: 0 Maximum value: 65535
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	-

Option	Description
enable	Enable L2TP client.
disable	Disable L2TP client.

security-mode	Turn on captive portal authentication for this interface.	option	-

Option	Description
none	No security option.
captive-portal	Captive portal authentication.
802.1X	802.1X port-based authentication.

Parameter	Description	Type	Size
security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-

Option	Description
mac-auth-only	Enable MAC authentication bypass without EAP.
enable	Enable MAC authentication bypass.
disable	Disable MAC authentication bypass.

security-8021x-mode *	802.1X mode.	option	-

Option	Description
default	802.1X default mode.
dynamic-vlan	802.1X dynamic VLAN (master) mode.
fallback	802.1X fallback (master) mode.
slave	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
security-external-web	URL of external authentication web server.	string	Maximum length: 127
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.	string	Maximum length: 127
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35
security-groups <name>	User groups that can authenticate with the captive portal. Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79
stp *	Enable/disable STP.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Disable STP. *enable* — Enable STP.		
stp-ha-slave *	Control STP behaviour on HA slave.	option	-
	Option / **Description** *disable* — Disable STP negotiation on HA slave. *enable* — Enable STP negotiation on HA slave. *priority-adjust* — Enable STP negotiation on HA slave and make priority lower than HA master.		
device-identification	Enable/disable passively gathering of device identity information about the devices on the network connected to this interface.	option	-
	Option / **Description** *enable* — Enable passive gathering of identity information about hosts. *disable* — 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	-
	Option / **Description** *enable* — Enable passive gathering of user identity information about users. *disable* — Disable passive gathering of user identity information about users.		
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-
	Option / **Description** *enable* — Enable reception of Link Layer Discovery Protocol (LLDP). *disable* — Disable reception of Link Layer Discovery Protocol (LLDP). *vdom* — Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable transmission of Link Layer Discovery Protocol (LLDP). *disable* / Disable transmission of Link Layer Discovery Protocol (LLDP). *vdom* / Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.		
lldp-network-policy	LLDP-MED network policy profile.	string	Maximum length: 35
broadcast-forticlient-discovery	Enable/disable broadcasting FortiClient discovery messages.	option	-
	Option / **Description** *enable* / Enable broadcasting FortiClient discovery messages. *disable* / Disable broadcasting FortiClient discovery messages.		
estimated-upstream-bandwidth	Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295
estimated-downstream-bandwidth	Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295
vrrp-virtual-mac	Enable/disable use of virtual MAC for VRRP.	option	-
	Option / **Description** *enable* / Enable use of virtual MAC for VRRP. *disable* / Disable use of virtual MAC for VRRP.		
role	Interface role.	option	-
	Option / **Description** *lan* / Connected to local network of endpoints. *wan* / Connected to Internet. *dmz* / Connected to server zone. *undefined* / Interface has no specific role.		

Parameter	Description	Type	Size
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 0 Maximum value: 4294967295
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-

Option	Description
enable	Enable secondary IP.
disable	Disable secondary IP.

Parameter	Description	Type	Size
preserve-session-route	Enable/disable preservation of session route when dirty.	option	-

Option	Description
enable	Enable preservation of session route when dirty.
disable	Disable preservation of session route when dirty.

Parameter	Description	Type	Size
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension device on this interface.	option	-

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.

Parameter	Description	Type	Size
ap-discover	Enable/disable automatic registration of unknown FortiAP devices.	option	-

Option	Description
enable	Enable automatic registration of unknown FortiAP devices.
disable	Disable automatic registration of unknown FortiAP devices.

Parameter	Description	Type	Size
fortilink-stacking	Enable/disable FortiLink switch-stacking on this interface.	option	-

Option	Description
enable	Enable FortiLink switch stacking.
disable	Disable FortiLink switch stacking.

Parameter	Description	Type	Size
fortilink-neighbor-detect	Protocol for FortiGate neighbor discovery.	option	-

Option	Description
lldp	Detect FortiLink neighbors using LLDP protocol.
fortilink	Detect FortiLink neighbors using FortiLink protocol.

fortilink-split-interface	Enable/disable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	option	-

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
fortilink-backup-link	fortilink split interface backup link.	integer	Minimum value: 0 Maximum value: 255
switch-controller-access-vlan	Block FortiSwitch port-to-port traffic.	option	-

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.

switch-controller-traffic-policy	Switch controller traffic policy for the VLAN.	string	Maximum length: 63
switch-controller-rspan-mode	Stop Layer2 MAC learning and interception of BPDUs and other packets on this interface.	option	-

Option	Description
disable	Disable RSPAN passthrough mode on this VLAN interface.
enable	Enable RSPAN passthrough mode on this VLAN interface.

Parameter	Description	Type	Size
switch-controller-igmp-snooping	Switch controller IGMP snooping.	option	-

Option	Description
enable	Enable IGMP snooping.
disable	Disable IGMP snooping.

Parameter	Description	Type	Size
switch-controller-igmp-snooping-proxy	Switch controller IGMP snooping proxy.	option	-

Option	Description
enable	Enable IGMP snooping proxy.
disable	Disable IGMP snooping proxy.

Parameter	Description	Type	Size
switch-controller-igmp-snooping-fast-leave	Switch controller IGMP snooping fast-leave.	option	-

Option	Description
enable	Enable IGMP snooping fast-leave.
disable	Disable IGMP snooping fast-leave.

Parameter	Description	Type	Size
switch-controller-dhcp-snooping	Switch controller DHCP snooping.	option	-

Option	Description
enable	Enable DHCP snooping for FortiSwitch devices.
disable	Disable DHCP snooping for FortiSwitch devices.

Parameter	Description	Type	Size
switch-controller-dhcp-snooping-verify-mac	Switch controller DHCP snooping verify MAC.	option	-

Option	Description
enable	Enable DHCP snooping verify source MAC for FortiSwitch devices.
disable	Disable DHCP snooping verify source MAC for FortiSwitch devices.

Parameter	Description	Type	Size
switch-controller-dhcp-snooping-option82	Switch controller DHCP snooping option82.	option	-

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

* This parameter may not exist in some models.

config l2tp-client-settings

Parameter	Description	Type	Size
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
peer-port	L2TP peer port number.	integer	Minimum value: 1 Maximum value: 65535
auth-type	L2TP authentication type.	option	-

Parameter	Description	Type	Size
	Option **Description** *auto* Automatically choose authentication. *pap* PAP authentication. *chap* CHAP authentication. *mschapv1* MS-CHAPv1 authentication. *mschapv2* MS-CHAPv2 authentication.		
mtu	L2TP MTU.	integer	Minimum value: 40 Maximum value: 65535
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295
defaultgw	Enable/disable default gateway.	option	-
	Option **Description** *enable* Enable default gateway. *disable* Disable default gateway.		
ip	IP.	ipv4-classnet-host	Not Specified

config vrrp

Parameter	Description	Type	Size
version	VRRP version.	option	-
	Option **Description** *2* VRRP version 2. *3* VRRP version 3.		

Parameter	Description	Type	Size
vrgrp	VRRP group ID .	integer	Minimum value: 1 Maximum value: 65535
vrip	IP address of the virtual router.	ipv4-address-any	Not Specified
priority	Priority of the virtual router .	integer	Minimum value: 1 Maximum value: 255
adv-interval	Advertisement interval .	integer	Minimum value: 1 Maximum value: 255
start-time	Startup time .	integer	Minimum value: 1 Maximum value: 255
preempt	Enable/disable preempt mode.	option	-

Option	Description
enable	Enable preempt mode.
disable	Disable preempt mode.

accept-mode	Enable/disable accept mode.	option	-

Option	Description
enable	Enable accept mode.
disable	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
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable ignoring of default route when checking destination. *disable* — Disable ignoring of default route when checking destination.		
status	Enable/disable this VRRP configuration.	option	-
	Option / **Description** *enable* — Enable this VRRP configuration. *disable* — Disable this VRRP configuration.		

config proxy-arp

Parameter	Description	Type	Size
ip	Set IP addresses of proxy ARP.	user	Not Specified

config secondaryip

Parameter	Description	Type	Size
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified
allowaccess	Management access settings for the secondary IP address.	option	-

Option	Description
ping	PING access.
https	HTTPS access.
ssh	SSH access.
snmp	SNMP access.
http	HTTP access.
telnet	TELNET access.
fgfm	FortiManager access.
radius-acct	RADIUS accounting access.
probe-response	Probe access.
fabric	Security Fabric access.
ftm	FTM access.

Parameter	Description	Type	Size
gwdetect	Enable/disable detect gateway alive for first.	option	-

Option	Description
enable	Enable detect gateway alive for first.
disable	Disable detect gateway alive for first.

ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255
detectserver	Gateway's ping server for this IP.	user	Not Specified
detectprotocol	Protocols used to detect the server.	option	-

Option	Description
ping	PING.
tcp-echo	TCP echo.
udp-echo	UDP echo.

ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50

config tagging

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

config ipv6

Parameter	Description	Type	Size
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-

Option	Description
static	Static setting.
dhcp	DHCPv6 client mode.

Parameter	Description	Type	Size
	Option / **Description** *pppoe* / IPv6 over PPPoE mode. *delegated* / IPv6 address with delegated prefix.		
nd-mode	Neighbor discovery mode.	option	-
	Option / **Description** *basic* / Do not support SEND. *SEND-compatible* / 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
nd-timestamp-delta	Neighbor discovery timestamp delta value .	integer	Minimum value: 1 Maximum value: 3600
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor .	integer	Minimum value: 1 Maximum value: 60
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-
	Option / **Description** *enable* / Enable using the DNS server acquired by DHCP. *disable* / Disable using the DNS server acquired by DHCP.		
ip6-address	Primary IPv6 address prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx	ipv6-prefix	Not Specified
ip6-allowaccess	Allow management access to the interface.	option	-

Parameter	Description	Type	Size
	Option **Description** *ping* PING access. *https* HTTPS access. *ssh* SSH access. *snmp* SNMP access. *http* HTTP access. *telnet* TELNET access. *fgfm* FortiManager access. *fabric* Fabric access.		
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-
	Option **Description** *enable* Enable sending advertisements about this interface. *disable* Disable sending advertisements about this interface.		
ip6-manage-flag	Enable/disable the managed flag.	option	-
	Option **Description** *enable* Enable the managed IPv6 flag. *disable* Disable the managed IPv6 flag.		
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-
	Option **Description** *enable* Enable the other IPv6 flag. *disable* Disable the other IPv6 flag.		
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350

Parameter	Description	Type	Size
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000
ip6-reachable-time	IPv6 reachable time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 3600000
ip6-retrans-time	IPv6 retransmit time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 4294967295
ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255
autoconf	Enable/disable address auto config.	option	-

Option	Description
enable	Enable auto-configuration.
disable	Disable auto-configuration.

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
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-

Option	Description
disable	Disable DHCPv6 relay
enable	Enable DHCPv6 relay.

dhcp6-relay-type	DHCPv6 relay type.	option	-

Parameter	Description	Type	Size
	Option **Description** *regular* Regular DHCP relay.		
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified
dhcp6-client-options	DHCPv6 client options.	option	-
	Option **Description** *rapid* Send rapid commit option. *iapd* Send including IA-PD option. *iana* Send including IA-NA option.		
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-
	Option **Description** *enable* Enable DHCPv6 prefix delegation. *disable* Disable DHCPv6 prefix delegation.		
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-
	Option **Description** *enable* Enable DHCPv6 information request. *disable* 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
dhcp6-prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 Maximum value: 4294967295
dhcp6-prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
vrrp-virtual-mac6	Enable/disable virtual MAC for VRRP.	option	-

Option	Description
enable	Enable virtual MAC for VRRP.
disable	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
autonomous-flag	Enable/disable the autonomous flag.	option	-

Option	Description
enable	Enable the autonomous flag.
disable	Disable the autonomous flag.

onlink-flag	Enable/disable the onlink flag.	option	-

Option	Description
enable	Enable the onlink flag.
disable	Disable the onlink flag.

valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295
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
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15
autonomous-flag	Enable/disable the autonomous flag.	option	-

Option	Description
enable	Enable the autonomous flag.
disable	Disable the autonomous flag.

Parameter	Description	Type	Size
onlink-flag	Enable/disable the onlink flag.	option	-

Option	Description
enable	Enable the onlink flag.
disable	Disable the onlink flag.

Parameter	Description	Type	Size
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified
rdnss-service	Recursive DNS service option.	option	-

Option	Description
delegated	Delegated RDNSS settings.
default	System RDNSS settings.
specify	Specify recursive DNS servers.

Parameter	Description	Type	Size
rdnss	Recursive DNS server option.	user	Not Specified

config vrrp6

Parameter	Description	Type	Size
vrgrp	VRRP group ID .	integer	Minimum value: 1 Maximum value: 65535
vrip6	IPv6 address of the virtual router.	ipv6-address	Not Specified
priority	Priority of the virtual router .	integer	Minimum value: 1 Maximum value: 255

Parameter	Description	Type	Size
adv-interval	Advertisement interval .	integer	Minimum value: 1 Maximum value: 255
start-time	Startup time .	integer	Minimum value: 1 Maximum value: 255
preempt	Enable/disable preempt mode.	option	-

Option	Description
enable	Enable preempt mode.
disable	Disable preempt mode.

accept-mode	Enable/disable accept mode.	option	-

Option	Description
enable	Enable accept mode.
disable	Disable accept mode.

vrdst6	Monitor the route to this destination.	ipv6-address	Not Specified
status	Enable/disable VRRP.	option	-

Option	Description
enable	Enable VRRP.
disable	Disable VRRP.

config system physical-switch

This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E. 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
age-enable	Enable/disable layer 2 age timer.	option	-
	Option / **Description** *enable* — Enable layer 2 ageing timer. *disable* — Disable layer 2 ageing timer.		
age-val	Layer 2 table age timer Value.	integer	Minimum value: 0 Maximum value: 4294967295

config system virtual-switch

This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E. 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}
      config port
         Description: Configure member ports.
         edit <name>
            set speed [auto|10full|...]
            set status [up|down]
            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
physical-switch	Physical switch parent.	string	Maximum length: 15
span	Enable/disable SPAN.	option	-

Option	Description
disable	Disable SPAN.
enable	Enable SPAN.

Parameter	Description	Type	Size
span-source-port	SPAN source ports.	string	Maximum length: 15
span-dest-port	SPAN destination port.	string	Maximum length: 15
span-direction	SPAN direction.	option	-

Option	Description
rx	Span receive direction only.
tx	Span transmit direction only.
both	Span both directions.

config port

Parameter	Description	Type	Size
speed	Interface speed.	option	-

Option	Description
auto	Automatically adjust speed.
10full	10M full-duplex.
10half	10M half-duplex.
100full	100M full-duplex.
100half	100M half-duplex.
1000full	1000M full-duplex.
1000half	1000M half-duplex.
1000auto	1000M auto adjust.

Parameter	Description	Type	Size
status	Interface status.	option	-

Parameter	Description	Type	Size
	Option / **Description** *up* / Interface up. *down* / Interface down.		
alias	Alias.	string	Maximum length: 25
poe *	Enable/disable PoE status. **Option** / **Description** *enable* / Enable PoE status. *disable* / Disable PoE status.	option	-

* This parameter may not exist in some models.

config system stp

This command is available for reference model(s) FortiGate 80E-POE, FortiWiFi 61E. 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
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	-

Parameter	Description	Type	Size
	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		
hello-time	Hello time .	integer	Minimum value: 1 Maximum value: 10
forward-delay	Forward delay .	integer	Minimum value: 4 Maximum value: 30
max-age	Maximum packet age .	integer	Minimum value: 6 Maximum value: 40
max-hops	Maximum number of hops .	integer	Minimum value: 1 Maximum value: 40

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 change-4-characters [enable|disable]
   set expire-status [enable|disable]
   set expire-day {integer}
   set reuse-password [enable|disable]
end
```

config system password-policy

Parameter	Description	Type	Size
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-

Option	Description
enable	Enable password policy.
disable	Disable password policy.

Parameter	Description	Type	Size
apply-to	Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.	option	-

Option	Description
admin-password	Apply to administrator passwords.
ipsec-preshared-key	Apply to IPsec pre-shared keys.

Parameter	Description	Type	Size
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128

Parameter	Description	Type	Size
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128
change-4-characters	Enable/disable changing at least 4 characters for a new password (This attribute overrides reuse-password if both are enabled).	option	-

Option	Description
enable	Enable requiring that at least 4 characters must be changed in a new password.
disable	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.

expire-status	Enable/disable password expiration.	option	-

Option	Description
enable	Passwords expire after expire-day days.
disable	Passwords do not expire.

expire-day	Number of days after which passwords expire .	integer	Minimum value: 1 Maximum value: 999
reuse-password	Enable/disable reusing of password (if both reuse-password and change-4-characters are enabled, change-4-characters overrides).	option	-

Option	Description
enable	Administrators are allowed to reuse the same password.
disable	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 change-4-characters [enable|disable]
   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
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-

Option	Description
enable	Enable password policy.
disable	Disable password policy.

Parameter	Description	Type	Size
apply-to	Guest administrator to which this password policy applies.	option	-

Option	Description
guest-admin-password	Apply to guest administrator password.

Parameter	Description	Type	Size
minimum-length	Minimum password length .	integer	Minimum value: 8 Maximum value: 128
min-lower-case-letter	Minimum number of lowercase characters in password .	integer	Minimum value: 0 Maximum value: 128

Parameter	Description	Type	Size
min-upper-case-letter	Minimum number of uppercase characters in password .	integer	Minimum value: 0 Maximum value: 128
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password .	integer	Minimum value: 0 Maximum value: 128
min-number	Minimum number of numeric characters in password .	integer	Minimum value: 0 Maximum value: 128
change-4-characters	Enable/disable changing at least 4 characters for a new password (This attribute overrides reuse-password if both are enabled).	option	-

Option	Description
enable	Enable requiring that at least 4 characters must be changed in a new password.
disable	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.

expire-status	Enable/disable password expiration.	option	-

Option	Description
enable	Passwords expire after expire-day days.
disable	Passwords do not expire.

expire-day	Number of days after which passwords expire .	integer	Minimum value: 1 Maximum value: 999
reuse-password	Enable/disable reusing of password (if both reuse-password and change-4-characters are enabled, change-4-characters overrides).	option	-

Option	Description
enable	Administrators are allowed to reuse the same password.
disable	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
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
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
wildcard	Enable/disable wildcard RADIUS authentication.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable username wildcard. *disable* / Disable username wildcard.		
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-
	Option / **Description** *enable* / Enable remote authentication. *disable* / 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	-
	Option / **Description** *enable* / Enable peer. *disable* / 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
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
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
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

Parameter	Description	Type	Size
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
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
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
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
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
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
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
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
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
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
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

Parameter	Description	Type	Size
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
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
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
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
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
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiGate features.	string	Maximum length: 35
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-

Option	Description
enable	Enable allow-remove option.
disable	Disable allow-remove option.

comments	Comment.	var-string	Maximum length: 255
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable access profile override.
disable	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	-

Option	Description
enable	Enable VDOM override.
disable	Disable VDOM override.

password-expire	Password expire time.	user	Not Specified
force-password-change	Enable/disable force password change on next login.	option	-

Option	Description
enable	Enable force password change on next login.
disable	Disable force password change on next login.

two-factor	Enable/disable two-factor authentication.	option	-

Option	Description
disable	Disable two-factor authentication.
fortitoken	Use FortiToken or FortiToken mobile two-factor authentication.
fortitoken-cloud	FortiToken Cloud Service.
email	Send a two-factor authentication code to the configured email-to email address.
sms	Send a two-factor authentication code to the configured sms-server and sms-phone.

Parameter	Description	Type	Size
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-

Option	Description
fortitoken	FortiToken authentication.
email	Email one time password.
sms	SMS one time password.

Parameter	Description	Type	Size
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-

Option	Description
email	Email notification for activation code.
sms	SMS notification for activation code.

Parameter	Description	Type	Size
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	-

Option	Description
fortiguard	Send SMS by FortiGuard.
custom	Send SMS by custom server.

Parameter	Description	Type	Size
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	-

Option	Description
disable	Disable guest authentication.
enable	Enable guest authentication.

Parameter	Description	Type	Size
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
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	-

Option	Description
enable	Enable peer.
disable	Disable peer.

Parameter	Description	Type	Size
peer-group	Peer group name.	string	Maximum length: 35

config trusthost

Parameter	Description	Type	Size
type	Trusthost type.	option	-

Option	Description
ipv4-trusthost	IPv4 trusthost.
ipv6-trusthost	IPv6 trusthost.

ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified

config system sso-admin

Configure SSO admin users.

```
config system sso-admin
   Description: Configure SSO admin users.
   edit <name>
      set accprofile {string}
      set vdom <name1>, <name2>, ...
   next
end
```

config system sso-admin

Parameter	Description	Type	Size
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 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 implicit-allow-dns [enable|disable]
set consolidated-firewall-mode [enable|disable]
set http-external-dest [fortiweb|forticache]
set firewall-session-dirty [check-all|check-new|...]
set manageip {user}
set gateway {ipv4-address}
set ip {ipv4-classnet-host}
set manageip6 {ipv6-prefix}
set gateway6 {ipv6-address}
set ip6 {ipv6-prefix}
set device {string}
set 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-nat46-64 [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-replacement-message-groups [enable|disable]
    set gui-voip-profile [enable|disable]
    set gui-ap-profile [enable|disable]
    set gui-dynamic-profile-display [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-multiple-utm-profiles [enable|disable]
    set gui-spamfilter [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-fortiap-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-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-domain-ip-reputation [enable|disable]
    set gui-multiple-interface-policy [enable|disable]
    set gui-per-policy-disclaimer [enable|disable]
    set ike-session-resume [enable|disable]
    set ike-quick-crash-detect [enable|disable]
    set ike-dn-format [with-space|no-space]
    set block-land-attack [disable|enable]
end
```

config system settings

Parameter	Description	Type	Size
comments	VDOM comments.	var-string	Maximum length: 255
opmode	Firewall operation mode (NAT or Transparent).	option	-

Option	Description
nat	Change to NAT mode.
transparent	Change to transparent mode.

Parameter	Description	Type	Size
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-

Option	Description
profile-based	Application and web-filtering are configured using profiles applied to policy entries.
policy-based	Application and web-filtering are configured as policy match conditions.

Parameter	Description	Type	Size
implicit-allow-dns	Enable/disable implicitly allowing DNS traffic.	option	-

Option	Description
enable	Enable implicitly allowing DNS traffic.
disable	Disable implicitly allowing DNS traffic.

Parameter	Description	Type	Size
consolidated-firewall-mode	Consolidated firewall mode.	option	-

Option	Description
enable	Enable consolidated firewall mode.
disable	Disable consolidated firewall mode.

Parameter	Description	Type	Size
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-

Option	Description
fortiweb	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.
forticache	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.

Parameter	Description	Type	Size
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-

Parameter	Description	Type	Size
	Option / **Description** *check-all* — All sessions affected by a firewall policy change are flushed from the session table. When new packets are recived they are re-evaluated by stateful inspection and re-added to the session table. *check-new* — Estabished sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration. *check-policy-option* — Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.		
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified
ip	IP address and netmask.	ipv4-classnet-host	Not Specified
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified
gateway6	Transparent mode IPv4 default gateway IP address.	ipv6-address	Not Specified
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified
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	-
	Option / **Description** *enable* — Enable Bi-directional Forwarding Detection (BFD) on all interfaces. *disable* — 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
bfd-required-min-rx	BFD required minimal receive interval .	integer	Minimum value: 1 Maximum value: 100000

Parameter	Description	Type	Size
bfd-detect-mult	BFD detection multiplier .	integer	Minimum value: 1 Maximum value: 50
bfd-dont-enforce-src-port	Enable to not enforce verifying the source port of BFD Packets.	option	-

Option	Description
enable	Enable verifying the source port of BFD Packets.
disable	Disable verifying the source port of BFD Packets.

Parameter	Description	Type	Size
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-

Option	Description
enable	Convert antispam tags to UTF-8.
disable	Do not convert antispam tags.

Parameter	Description	Type	Size
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-

Option	Description
enable	Enable WCCP cache engine.
disable	Disable WCCP cache engine.

Parameter	Description	Type	Size
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-

Option	Description
ipsec	IPsec.
pptp	PPTP.
l2tp	L2TP.
ssl	SSL.

Parameter	Description	Type	Size
vpn-stats-period	Period to send VPN log statistics .	integer	Minimum value: 0 Maximum value: 4294967295
v4-ecmp-mode	IPv4 Equal-cost multi-path (ECMP) routing and load balancing mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *source-ip-based* / Select next hop based on source IP. *weight-based* / Select next hop based on weight. *usage-based* / Select next hop based on usage. *source-dest-ip-based* / 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
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiGate.	option	-
	Option / **Description** *enable* / Perform a policy check every time. *disable* / Perform a policy check only the first time the session is received.		
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-
	Option / **Description** *enable* / Try to keep PRP trailer. *disable* / Trim PRP trailer.		
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-
	Option / **Description** *enable* / Enable SNAT for hairpin traffic. *disable* / Disable SNAT for hairpin traffic.		
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-
	Option / **Description** *enable* / Enable the DHCP proxy. *disable* / Disable the DHCP proxy.		

Parameter	Description	Type	Size
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	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	-

Option	Description
enable	Enable central NAT.
disable	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	-

Option	Description
enable	Enable LLDP reception for this VDOM.
disable	Disable LLDP reception for this VDOM.
global	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	-

Option	Description
enable	Enable LLDP transmission for this VDOM.
disable	Disable LLDP transmission for this VDOM.
global	Use the global LLDP transmission configuration for this VDOM.

Parameter	Description	Type	Size
link-down-access	Enable/disable link down access traffic.	option	-

Option	Description
enable	Allow link down access traffic.
disable	Block link down access traffic.

Parameter	Description	Type	Size
auxiliary-session	Enable/disable auxiliary session.	option	-

Option	Description
enable	Enable auxiliary session for this VDOM.
disable	Disable auxiliary session for this VDOM.

Parameter	Description	Type	Size
asymroute	Enable/disable IPv4 asymmetric routing.	option	-

Option	Description
enable	Enable IPv4 asymmetric routing.
disable	Disable IPv4 asymmetric routing.

Parameter	Description	Type	Size
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-

Option	Description
enable	Enable ICMP asymmetric routing.
disable	Disable ICMP asymmetric routing.

Parameter	Description	Type	Size
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-

Option	Description
enable	Allow TCP session without SYN flags.
disable	Do not allow TCP session without SYN flags.

Parameter	Description	Type	Size
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-

Option	Description
enable	Include denied sessions in the session table.
disable	Do not add denied sessions to the session table.

Parameter	Description	Type	Size
strict-src-check	Enable/disable strict source verification.	option	-

Option	Description
enable	Enable strict source verification.
disable	Disable strict source verification.

Parameter	Description	Type	Size
allow-linkdown-path	Enable/disable link down path.	option	-

Option	Description
enable	Allow link down path.
disable	Do not allow link down path.

Parameter	Description	Type	Size
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-

Option	Description
enable	Enable asymmetric IPv6 routing.
disable	Disable asymmetric IPv6 routing.

Parameter	Description	Type	Size
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-

Option	Description
enable	Enable asymmetric ICMPv6 routing.
disable	Disable asymmetric ICMPv6 routing.

Parameter	Description	Type	Size
sctp-session-without-init	Enable/disable SCTP session creation without SCTP INIT.	option	-

Option	Description
enable	Enable SCTP session creation without SCTP INIT.
disable	Disable SCTP session creation without SCTP INIT.

Parameter	Description	Type	Size
sip-expectation	Enable/disable the SIP kernel session helper to create an expectation for port 5060.	option	-

Option	Description
enable	Allow SIP session helper to create an expectation for port 5060.
disable	Prevent SIP session helper from creating an expectation for port 5060.

Parameter	Description	Type	Size
sip-nat-trace	Enable/disable recording the original SIP source IP address when NAT is used.	option	-

Option	Description
enable	Record the original SIP source IP address when NAT is used.
disable	Do not record the original SIP source IP address when NAT is used.

Parameter	Description	Type	Size
status	Enable/disable this VDOM.	option	-

Option	Description
enable	Enable this VDOM.
disable	Disable this VDOM.

Parameter	Description	Type	Size
sip-tcp-port	TCP port the SIP proxy monitors for SIP traffic .	integer	Minimum value: 1 Maximum value: 65535
sip-udp-port	UDP port the SIP proxy monitors for SIP traffic .	integer	Minimum value: 1 Maximum value: 65535
sip-ssl-port	TCP port the SIP proxy monitors for SIP SSL/TLS traffic .	integer	Minimum value: 0 Maximum value: 65535
sccp-port	TCP port the SCCP proxy monitors for SCCP traffic .	integer	Minimum value: 0 Maximum value: 65535
multicast-forward	Enable/disable multicast forwarding.	option	-

Option	Description
enable	Enable multicast forwarding.
disable	Disable multicast forwarding.

Parameter	Description	Type	Size
multicast-ttl-notchange	Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / The multicast TTL is not changed. *disable* / The multicast TTL may be changed.		
multicast-skip-policy	Enable/disable allowing multicast traffic through the FortiGate without a policy check.	option	-
	Option / **Description** *enable* / Allowing multicast traffic through the FortiGate without creating a multicast firewall policy. *disable* / 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	-
	Option / **Description** *enable* / Enable overlapping subnets. *disable* / Disable overlapping subnets.		
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-
	Option / **Description** *enable* / Deny TCP with ICMP. *disable* / Disable denying TCP with ICMP.		
ecmp-max-paths	Maximum number of Equal Cost Multi-Path .	integer	Minimum value: 1 Maximum value: 255
discovered-device-timeout	Timeout for discovered devices .	integer	Minimum value: 1 Maximum value: 365
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-
	Option / **Description** *disable* / Disable email address checking with DNS. *enable* / Enable email address checking with DNS.		

Parameter	Description	Type	Size
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	-

Option	Description
proxy-based	Use a default proxy-based VoIP ALG.
kernel-helper-based	Use the SIP session helper.

Parameter	Description	Type	Size
gui-icap	Enable/disable ICAP on the GUI.	option	-

Option	Description
enable	Enable ICAP on the GUI.
disable	Disable ICAP on the GUI.

Parameter	Description	Type	Size
gui-nat46-64	Enable/disable NAT46 and NAT64 settings on the GUI.	option	-

Option	Description
enable	Enable NAT46 and NAT64 settings on the GUI.
disable	Disable NAT46 and NAT64 settings on the GUI.

Parameter	Description	Type	Size
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-

Option	Description
enable	Enable implicit firewall policies on the GUI.
disable	Disable implicit firewall policies on the GUI.

Parameter	Description	Type	Size
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-

Option	Description
enable	Enable DNS database settings on the GUI.
disable	Disable DNS database settings on the GUI.

Parameter	Description	Type	Size
gui-load-balance	Enable/disable server load balancing on the GUI.	option	-

Option	Description
enable	Enable server load balancing on the GUI.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable server load balancing on the GUI.		
gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-
	Option **Description** *enable* Enable multicast firewall policies on the GUI. *disable* Disable multicast firewall policies on the GUI.		
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-
	Option **Description** *enable* Enable DoS policies on the GUI. *disable* Disable DoS policies on the GUI.		
gui-object-colors	Enable/disable object colors on the GUI.	option	-
	Option **Description** *enable* Enable object colors on the GUI. *disable* Disable object colors on the GUI.		
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-
	Option **Description** *enable* Enable replacement message groups on the GUI. *disable* Disable replacement message groups on the GUI.		
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-
	Option **Description** *enable* Enable VoIP profiles on the GUI. *disable* Disable VoIP profiles on the GUI.		
gui-ap-profile	Enable/disable FortiAP profiles on the GUI.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable FortiAP profiles on the GUI. *disable* Disable FortiAP profiles on the GUI.		
gui-dynamic-profile-display	Enable/disable RADIUS Single Sign On (RSSO) on the GUI.	option	-
	Option **Description** *enable* Enable RADIUS Single Sign On (RSSO) on the GUI. *disable* Disable RADIUS Single Sign On (RSSO) on the GUI.		
gui-local-in-policy	Enable/disable Local-In policies on the GUI.	option	-
	Option **Description** *enable* Enable Local-In policies on the GUI. *disable* Disable Local-In policies on the GUI.		
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-
	Option **Description** *enable* Enable the explicit proxy on the GUI. *disable* Disable the explicit proxy on the GUI.		
gui-dynamic-routing	Enable/disable dynamic routing on the GUI.	option	-
	Option **Description** *enable* Enable dynamic routing on the GUI. *disable* Disable dynamic routing on the GUI.		
gui-sslvpn-personal-bookmarks	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-
	Option **Description** *enable* Enable SSL-VPN personal bookmark management on the GUI. *disable* Disable SSL-VPN personal bookmark management on the GUI.		

Parameter	Description	Type	Size
gui-sslvpn-realms	Enable/disable SSL-VPN realms on the GUI.	option	-

Option	Description
enable	Enable SSL-VPN realms on the GUI.
disable	Disable SSL-VPN realms on the GUI.

Parameter	Description	Type	Size
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-

Option	Description
enable	Enable policy-based IPsec VPN on the GUI.
disable	Disable policy-based IPsec VPN on the GUI.

Parameter	Description	Type	Size
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-

Option	Description
enable	Enable threat weight on the GUI.
disable	Disable threat weight on the GUI.

Parameter	Description	Type	Size
gui-multiple-utm-profiles	Enable/disable multiple UTM profiles on the GUI.	option	-

Option	Description
enable	Enable multiple UTM profiles on the GUI.
disable	Disable multiple UTM profiles on the GUI.

Parameter	Description	Type	Size
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-

Option	Description
enable	Enable Antispam on the GUI.
disable	Disable Antispam on the GUI.

Parameter	Description	Type	Size
gui-application-control	Enable/disable application control on the GUI.	option	-

Option	Description
enable	Enable application control on the GUI.
disable	Disable application control on the GUI.

Parameter	Description	Type	Size
gui-ips	Enable/disable IPS on the GUI.	option	-

Option	Description
enable	Enable IPS on the GUI.
disable	Disable IPS on the GUI.

Parameter	Description	Type	Size
gui-endpoint-control	Enable/disable endpoint control on the GUI.	option	-

Option	Description
enable	Enable endpoint control on the GUI.
disable	Disable endpoint control on the GUI.

Parameter	Description	Type	Size
gui-endpoint-control-advanced	Enable/disable advanced endpoint control options on the GUI.	option	-

Option	Description
enable	Enable advanced endpoint control options on the GUI.
disable	Disable advanced endpoint control options on the GUI.

Parameter	Description	Type	Size
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-

Option	Description
enable	Enable advanced DHCP options on the GUI.
disable	Disable advanced DHCP options on the GUI.

Parameter	Description	Type	Size
gui-vpn	Enable/disable VPN tunnels on the GUI.	option	-

Option	Description
enable	Enable VPN tunnels on the GUI.
disable	Disable VPN tunnels on the GUI.

Parameter	Description	Type	Size
gui-wireless-controller	Enable/disable the wireless controller on the GUI.	option	-

Option	Description
enable	Enable the wireless controller on the GUI.
disable	Disable the wireless controller on the GUI.

Parameter	Description	Type	Size
gui-switch-controller	Enable/disable the switch controller on the GUI.	option	-

Option	Description
enable	Enable the switch controller on the GUI.
disable	Disable the switch controller on the GUI.

Parameter	Description	Type	Size
gui-fortiap-split-tunneling	Enable/disable FortiAP split tunneling on the GUI.	option	-

Option	Description
enable	Enable FortiAP split tunneling on the GUI.
disable	Disable FortiAP split tunneling on the GUI.

Parameter	Description	Type	Size
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-

Option	Description
enable	Enable advanced web filtering on the GUI.
disable	Disable advanced web filtering on the GUI.

Parameter	Description	Type	Size
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-

Option	Description
enable	Enable traffic shaping on the GUI.
disable	Disable traffic shaping on the GUI.

Parameter	Description	Type	Size
gui-wan-load-balancing	Enable/disable SD-WAN on the GUI.	option	-

Option	Description
enable	Enable SD-WAN on the GUI.
disable	Disable SD-WAN on the GUI.

Parameter	Description	Type	Size
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-

Option	Description
enable	Enable AntiVirus on the GUI.
disable	Disable AntiVirus on the GUI.

Parameter	Description	Type	Size
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-

Option	Description
enable	Enable Web filtering on the GUI.
disable	Disable Web filtering on the GUI.

Parameter	Description	Type	Size
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-

Option	Description
enable	Enable DNS Filtering on the GUI.
disable	Disable DNS Filtering on the GUI.

Parameter	Description	Type	Size
gui-waf-profile	Enable/disable Web Application Firewall on the GUI.	option	-

Option	Description
enable	Enable Web Application Firewall on the GUI.
disable	Disable Web Application Firewall on the GUI.

Parameter	Description	Type	Size
gui-fortiextender-controller	Enable/disable FortiExtender on the GUI.	option	-

Option	Description
enable	Enable FortiExtender on the GUI.
disable	Disable FortiExtender on the GUI.

Parameter	Description	Type	Size
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-

Option	Description
enable	Enable advanced policy configuration on the GUI.
disable	Disable advanced policy configuration on the GUI.

Parameter	Description	Type	Size
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-

Option	Description
enable	Enable the requirement for policy naming on the GUI.
disable	Disable the requirement for policy naming on the GUI.

Parameter	Description	Type	Size
gui-email-collection	Enable/disable email collection on the GUI.	option	-

Option	Description
enable	Enable email collection on the GUI.
disable	Disable email collection on the GUI.

Parameter	Description	Type	Size
gui-domain-ip-reputation	Enable/disable Domain and IP Reputation on the GUI.	option	-

Option	Description
enable	Enable Domain and IP Reputation on the GUI.
disable	Disable Domain and IP Reputation on the GUI.

Parameter	Description	Type	Size
gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-

Option	Description
enable	Enable adding multiple interfaces to a policy on the GUI.
disable	Disable adding multiple interfaces to a policy on the GUI.

Parameter	Description	Type	Size
gui-per-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-

Option	Description
enable	Enable policy disclaimer on the GUI.
disable	Disable policy disclaimer on the GUI.

Parameter	Description	Type	Size
ike-session-resume	Enable/disable IKEv2 session resumption (RFC 5723).	option	-

Option	Description
enable	Enable IKEv2 session resumption (RFC 5723).
disable	Disable IKEv2 session resumption (RFC 5723).

Parameter	Description	Type	Size
ike-quick-crash-detect	Enable/disable IKE quick crash detection (RFC 6290).	option	-

Option	Description
enable	Enable IKE quick crash detection (RFC 6290).
disable	Disable IKE quick crash detection (RFC 6290).

Parameter	Description	Type	Size
ike-dn-format	Configure IKE ASN.1 Distinguished Name format conventions.	option	-

Option	Description
with-space	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.
no-space	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.

Parameter	Description	Type	Size
block-land-attack	Enable/disable blocking of land attacks.	option	-

Option	Description
disable	Do not block land attack.
enable	Block land attack.

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 auto-asic-offload [enable|disable]
   next
end
```

config system sit-tunnel

Parameter	Description	Type	Size
source	Source IP address of the tunnel.	ipv4-address	Not Specified
destination	Destination IP address of the tunnel.	ipv4-address	Not Specified
ip6	IPv6 address of the tunnel.	ipv6-prefix	Not Specified
interface	Interface name.	string	Maximum length: 15

Parameter	Description	Type	Size
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-

Option	Description
enable	Enable auto ASIC offloading.
disable	Disable ASIC offloading.

* This parameter may not exist in some models.

config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fsso-polling
   Description: Configure Fortinet Single Sign On (FSSO) server.
   set status [enable|disable]
   set listening-port {integer}
   set authentication [enable|disable]
   set auth-password {password}
end
```

config system fsso-polling

Parameter	Description	Type	Size
status	Enable/disable FSSO Polling Mode.	option	-

Option	Description
enable	Enable FSSO Polling Mode.
disable	Disable FSSO Polling Mode.

listening-port	Listening port to accept clients .	integer	Minimum value: 1 Maximum value: 65535
authentication	Enable/disable FSSO Agent Authentication.	option	-

Option	Description
enable	Enable FSSO Agent Authentication.
disable	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-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 uninterruptible-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-uptime-diff-margin {integer}
   set standalone-config-sync [enable|disable]
   set logical-sn [enable|disable]
   set vcluster2 [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-slave-force-reset [enable|disable]
    set pingserver-flip-timeout {integer}
    set vdom {user}
    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-slave-force-reset [enable|disable]
       set vdom {user}
    end
    set ha-direct [enable|disable]
    set ssd-failover [enable|disable]
    set memory-compatible-mode [enable|disable]
    set inter-cluster-session-sync [enable|disable]
end
```

config system ha

Parameter	Description	Type	Size
group-id	Cluster group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255
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	-

Option	Description
standalone	Standalone mode.

Parameter	Description	Type	Size
	Option **Description** *a-a* Active-active mode. *a-p* Active-passive mode.		
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-
	Option **Description** *enable* Enable HA packet distribution to multiple CPUs. *disable* 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
route-wait	Time to wait before sending new routes to the cluster .	integer	Minimum value: 0 Maximum value: 3600
route-hold	Time to wait between routing table updates to the cluster .	integer	Minimum value: 0 Maximum value: 3600
multicast-ttl	HA multicast TTL on master .	integer	Minimum value: 5 Maximum value: 3600
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-
	Option **Description** *enable* Enable load balance.		

Parameter	Description	Type	Size
	Option **Description** *disable* Disable load balance.		
sync-config	Enable/disable configuration synchronization.	option	-
	Option **Description** *enable* Enable configuration synchronization. *disable* Disable configuration synchronization.		
encryption	Enable/disable heartbeat message encryption.	option	-
	Option **Description** *enable* Enable heartbeat message encryption. *disable* Disable heartbeat message encryption.		
authentication	Enable/disable heartbeat message authentication.	option	-
	Option **Description** *enable* Enable heartbeat message authentication. *disable* Disable heartbeat message authentication.		
hb-interval	Time between sending heartbeat packets . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20
hb-lost-threshold	Number of lost heartbeats to signal a failure . Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60
hello-holddown	Time to wait before changing from hello to work state .	integer	Minimum value: 5 Maximum value: 300
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-
	Option **Description** *enable* Enable gratuitous ARPs. *disable* Disable gratuitous ARPs.		

Parameter	Description	Type	Size
arps	Number of gratuitous ARPs . Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60
arps-interval	Time between gratuitous ARPs . Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20
session-pickup	Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.	option	-

Option	Description
enable	Enable session pickup.
disable	Disable session pickup.

Parameter	Description	Type	Size
session-pickup-connectionless	Enable/disable UDP and ICMP session sync.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
session-pickup-expectation	Enable/disable session helper expectation session sync for FGSP.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
session-pickup-nat	Enable/disable NAT session sync for FGSP.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
session-pickup-delay	Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* 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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
standalone-mgmt-vdom	Enable/disable standalone management VDOM.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ha-eth-type	HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4
hc-eth-type	Transparent mode HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4
l2ep-eth-type	Telnet session HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4

Parameter	Description	Type	Size
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535
standalone-config-sync	Enable/disable FGSP configuration synchronization.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
logical-sn	Enable/disable usage of the logical serial number.	option	-

Option	Description
enable	Enable usage of the logical serial number.
disable	Disable usage of the logical serial number.

Parameter	Description	Type	Size
vcluster2	Enable/disable virtual cluster 2 for virtual clustering.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255
override	Enable and increase the priority of the unit that should always be primary (master).	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255

Parameter	Description	Type	Size
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600
schedule	Type of A-A load balancing. Use none if you have external load balancers.	option	-

Option	Description
none	None.
hub	Hub.
leastconnection	Least connection.
round-robin	Round robin.
weight-round-robin	Weight round robin.
random	Random.
ip	IP.
ipport	IP port.

weight	Weight-round-robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified
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

Parameter	Description	Type	Size
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
pingserver-slave-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-

Option	Description
enable	Enable force reset of slave after PING server failure.
disable	Disable force reset of slave 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
vdom	VDOMs in virtual cluster 1.	user	Not Specified
ha-direct	Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, and FortiSandbox.	option	-

Option	Description
enable	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.
disable	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.

ssd-failover	Enable/disable automatic HA failover on SSD disk failure.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

memory-compatible-mode	Enable/disable memory compatible mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
inter-cluster-session-sync	Enable/disable synchronization of sessions among HA clusters.	option	-
	Option / **Description** *enable* / Enable synchronization of sessions among HA clusters. *disable* / Disable synchronization of sessions among HA clusters.		

config ha-mgmt-interfaces

Parameter	Description	Type	Size
interface	Interface to reserve for HA management.	string	Maximum length: 15
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified
gateway	Default route gateway for reserved HA management interface.	ipv4-address	Not Specified
gateway6	Default IPv6 gateway for reserved HA management interface.	ipv6-address	Not Specified

config secondary-vcluster

Parameter	Description	Type	Size
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255
override	Enable and increase the priority of the unit that should always be primary (master).	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
priority	Increase the priority to select the primary unit .	integer	Minimum value: 0 Maximum value: 255

Parameter	Description	Type	Size
override-wait-time	Delay negotiating if override is enabled . Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600
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
pingserver-slave-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-

Option	Description
enable	Enable force reset of slave after PING server failure.
disable	Disable force reset of slave 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
monitor-vlan	Enable/disable monitor VLAN interfaces.	option	-

Option	Description
enable	Enable monitor VLAN interfaces.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable monitor VLAN interfaces.		
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30
vlan-hb-lost-threshold	VLAN lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 60

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
status	Enable/disable storage.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
media-status	The physical status of current media.	option	-
	Option **Description** *enable* Storage is enabled. *disable* Storage is disabled.		

Parameter	Description	Type	Size
	Option / **Description** *fail* / Storage have some fail sector.		
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255
partition	Label of underlying partition.	string	Maximum length: 16
device	Partition device.	string	Maximum length: 19
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295
usage	Use hard disk for logging and WAN Optimization.	option	-
	Option / **Description** *log* / 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
status	Enable/disable dedicated management.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
interface	Dedicated management interface.	string	Maximum length: 15
default-gateway	Default gateway for dedicated management interface.	ipv4-address	Not Specified
dhcp-server	Enable/disable DHCP server on management interface.	option	-
	Option **Description** *enable* Enable DHCP server on management port. *disable* Disable DHCP server on management port.		
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified

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
interface	Interface name.	string	Maximum length: 15
ip	IP address.	ipv4-address	Not Specified
mac	MAC address.	mac-address	Not Specified

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
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

config system dns

Configure DNS.

```
config system dns
   Description: Configure DNS.
   set primary {ipv4-address}
   set secondary {ipv4-address}
   set dns-over-tls [disable|enable|...]
   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}
end
```

config system dns

Parameter	Description	Type	Size
primary	Primary DNS server IP address.	ipv4-address	Not Specified
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified
dns-over-tls	Enable/disable/enforce DNS over TLS.	option	-

Option	Description
disable	Disable DNS over TLS.
enable	Use TLS for DNS queries if TLS is available.
enforce	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.

ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35
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
retry	Number of times to retry .	integer	Minimum value: 0 Maximum value: 5
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400

Parameter	Description	Type	Size
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-

Option	Description
disable	Disable cache NOTFOUND responses from DNS server.
enable	Enable cache NOTFOUND responses from DNS server.

Parameter	Description	Type	Size
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

config system ddns

Configure DDNS.

```
config system ddns
   Description: Configure DDNS.
   edit <ddnsid>
      set ddns-server [dyndns.org|dyns.net|...]
      set ddns-server-ip {ipv4-address}
      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 update-interval {integer}
      set clear-text [disable|enable]
      set ssl-certificate {string}
      set bound-ip {ipv4-address}
      set monitor-interface <interface-name1>, <interface-name2>, ...
   next
end
```

config system ddns

Parameter	Description	Type	Size
ddns-server	Select a DDNS service provider.	option	-

Option	Description
dyndns.org	members.dyndns.org and dnsalias.com
dyns.net	www.dyns.net
tzo.com	rh.tzo.com
vavic.com	Peanut Hull
dipdns.net	dipdnsserver.dipdns.com
now.net.cn	ip.todayisp.com
dhs.org	members.dhs.org
easydns.com	members.easydns.com
genericDDNS	Generic DDNS based on RFC2136.
FortiGuardDDNS	FortiGuard DDNS service.
noip.com	dynupdate.no-ip.com

ddns-server-ip	Generic DDNS server IP.	ipv4-address	Not Specified
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
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-

Option	Description
disable	Disable DDNS authentication.
tsig	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

Parameter	Description	Type	Size
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	-

Option	Description
disable	Disable use of public IP address.
enable	Enable use of public IP address.

update-interval	DDNS update interval .	integer	Minimum value: 60 Maximum value: 2592000
clear-text	Enable/disable use of clear text connections.	option	-

Option	Description
disable	Disable use of clear text connections.
enable	Enable use of clear text connections.

ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35
bound-ip	Bound IP address.	ipv4-address	Not Specified
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}
end
```

config system sflow

Parameter	Description	Type	Size
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
collector-port	UDP port number used for sending sFlow datagrams .	integer	Minimum value: 0 Maximum value: 65535
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified

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}
end
```

config system vdom-sflow

Parameter	Description	Type	Size
vdom-sflow	Enable/disable the sFlow configuration for the current VDOM.	option	-
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
collector-port	UDP port number used for sending sFlow datagrams .	integer	Minimum value: 0 Maximum value: 65535
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified

Option	Description
enable	Enable sFlow for this VDOM.
disable	Disable sFlow for this VDOM.

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}
end
```

config system netflow

Parameter	Description	Type	Size
collector-ip	Collector IP.	ipv4-address	Not Specified
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified
active-flow-timeout	Timeout to report active flows .	integer	Minimum value: 1 Maximum value: 60
inactive-flow-timeout	Timeout for periodic report of finished flows .	integer	Minimum value: 10 Maximum value: 600
template-tx-timeout	Timeout for periodic template flowset transmission .	integer	Minimum value: 1 Maximum value: 1440
template-tx-counter	Counter of flowset records before resending a template flowset record.	integer	Minimum value: 10 Maximum value: 6000

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}
end
```

config system vdom-netflow

Parameter	Description	Type	Size
vdom-netflow	Enable/disable NetFlow per VDOM.	option	-
	Option / **Description** *enable* / Enable NetFlow per VDOM. *disable* / Disable NetFlow per VDOM.		
collector-ip	NetFlow collector IP address.	ipv4-address	Not Specified
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified

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 dns-over-tls [disable|enable|...]
   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}
end
```

config system vdom-dns

Parameter	Description	Type	Size
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-

Option	Description
enable	Enable configuring DNS servers for the current VDOM.
disable	Disable configuring DNS servers for the current VDOM.

primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified
dns-over-tls	Enable/disable/enforce DNS over TLS.	option	-

Option	Description
disable	Disable DNS over TLS.
enable	Use TLS for DNS queries if TLS is available.
enforce	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.

ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35
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
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

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

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
image-type	Image type.	option	-
	Option / **Description**: *gif* — GIF image.; *jpg* — JPEG image.; *tiff* — TIFF image.; *png* — 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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.

Parameter	Description	Type	Size
	Option **Description** *http* HTTP *8bit* 8 bit.		
format	Format flag.	option	-
	Option **Description** *none* No format type. *text* Text format. *html* HTML format.		

config system replacemsg webproxy

Replacement messages.

```
config system replacemsg webproxy
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg webproxy

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-
	Option **Description** *none* No header type. *http* HTTP *8bit* 8 bit.		
format	Format flag.	option	-

Parameter	Description	Type	Size

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg ftp

Replacement messages.

```
config system replacemsg ftp
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg ftp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg nntp

Replacement messages.

```
config system replacemsg nntp
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg nntp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.

Parameter	Description	Type	Size
	Option / **Description** *http* / HTTP *8bit* / 8 bit.		
format	Format flag.	option	-
	Option / **Description** *none* / No format type. *text* / Text format. *html* / HTML format.		

config system replacemsg alertmail

Replacement messages.

```
config system replacemsg alertmail
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg alertmail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-
	Option / **Description** *none* / No header type. *http* / HTTP *8bit* / 8 bit.		
format	Format flag.	option	-

Parameter	Description	Type	Size

Option	Description
none	No format type.
text	Text format.
html	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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg auth

Replacement messages.

```
config system replacemsg auth
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg auth

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg device-detection-portal

Replacement messages.

```
config system replacemsg device-detection-portal
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg device-detection-portal

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.

Parameter	Description	Type	Size
	Option **Description** *http* HTTP *8bit* 8 bit.		
format	Format flag.	option	-
	Option **Description** *none* No format type. *text* Text format. *html* 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
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-
	Option **Description** *none* No header type. *http* HTTP *8bit* 8 bit.		
format	Format flag.	option	-

Parameter	Description	Type	Size

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg traffic-quota

Replacement messages.

```
config system replacemsg traffic-quota
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg traffic-quota

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg utm

Replacement messages.

```
config system replacemsg utm
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg utm

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg icap

Replacement messages.

```
config system replacemsg icap
   Description: Replacement messages.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
```

config system replacemsg icap

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config system replacemsg-group

Configure replacement message groups.

```
config system replacemsg-group
   Description: Configure replacement message groups.
   edit <name>
      set comment {var-string}
      set group-type [default|utm|...]
      config mail
         Description: Replacement message table entries.
         edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
         next
      end
      config http
         Description: Replacement message table entries.
         edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
         next
      end
      config webproxy
         Description: Replacement message table entries.
         edit <msg-type>
            set buffer {var-string}
```

```
      set header [none|http|...]
      set format [none|text|...]
   next
end
config ftp
   Description: Replacement message table entries.
   edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
   next
end
config nntp
   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 device-detection-portal
   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
  next
end
```

config system replacemsg-group

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
group-type	Group type.	option	-

Option	Description
default	Per-vdom replacement messages.
utm	For use with UTM settings in firewall policies.
auth	For use with authentication pages in firewall policies.

config mail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config http

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config webproxy

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config ftp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config nntp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config fortiguard-wf

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config spam

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config alertmail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config admin

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config auth

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config sslvpn

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config device-detection-portal

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config nac-quar

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config traffic-quota

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config utm

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config custom-message

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	HTML format.

config icap

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
header	Header flag.	option	-

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size
format	Format flag.	option	-

Option	Description
none	No format type.
text	Text format.
html	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 {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
status	Enable/disable SNMP.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
engine-id	Local SNMP engineID string (maximum 24 characters).	string	Maximum length: 24
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
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100

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
name	Community name.	string	Maximum length: 35
status	Enable/disable this SNMP community.	option	-

Option	Description
enable	Enable setting.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable setting.		
query-v1-status	Enable/disable SNMP v1 queries.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
query-v1-port	SNMP v1 query port .	integer	Minimum value: 1 Maximum value: 65535
query-v2c-status	Enable/disable SNMP v2c queries.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
query-v2c-port	SNMP v2c query port .	integer	Minimum value: 0 Maximum value: 65535
trap-v1-status	Enable/disable SNMP v1 traps.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
trap-v1-lport	SNMP v1 trap local port .	integer	Minimum value: 1 Maximum value: 65535
trap-v1-rport	SNMP v1 trap remote port .	integer	Minimum value: 1 Maximum value: 65535
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
trap-v2c-lport	SNMP v2c trap local port .	integer	Minimum value: 1 Maximum value: 65535
trap-v2c-rport	SNMP v2c trap remote port .	integer	Minimum value: 1 Maximum value: 65535
events	SNMP trap events.	option	-
	Option / **Description** *cpu-high* / Send a trap when CPU usage is high. *mem-low* / Send a trap when available memory is low. *log-full* / Send a trap when log disk space becomes low. *intf-ip* / Send a trap when an interface IP address is changed. *vpn-tun-up* / Send a trap when a VPN tunnel comes up. *vpn-tun-down* / Send a trap when a VPN tunnel goes down. *ha-switch* / Send a trap after an HA failover when the backup unit has taken over. *ha-hb-failure* / Send a trap when HA heartbeats are not received. *ips-signature* / Send a trap when IPS detects an attack. *ips-anomaly* / Send a trap when IPS finds an anomaly. *av-virus* / Send a trap when AntiVirus finds a virus. *av-oversize* / Send a trap when AntiVirus finds an oversized file. *av-pattern* / Send a trap when AntiVirus finds file matching pattern. *av-fragmented* / Send a trap when AntiVirus finds a fragmented file. *fm-if-change* / Send a trap when FortiManager interface changes. Send a FortiManager trap. *fm-conf-change* / Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager. *bgp-established* / Send a trap when a BGP FSM transitions to the established state.		

Parameter	Description	Type	Size

Option	Description
bgp-backward-transition	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
ha-member-up	Send a trap when an HA cluster member goes up.
ha-member-down	Send a trap when an HA cluster member goes down.
ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).
av-conserve	Send a trap when the FortiGate enters conserve mode.
av-bypass	Send a trap when the FortiGate enters bypass mode.
av-oversize-passed	Send a trap when AntiVirus passes an oversized file.
av-oversize-blocked	Send a trap when AntiVirus blocks an oversized file.
ips-pkg-update	Send a trap when the IPS signature database or engine is updated.
ips-fail-open	Send a trap when the IPS network buffer is full.
faz-disconnect	Send a trap when a FortiAnalyzer disconnects from the FortiGate.
wc-ap-up	Send a trap when a managed FortiAP comes up.
wc-ap-down	Send a trap when a managed FortiAP goes down.
fswctl-session-up	Send a trap when a FortiSwitch controller session comes up.
fswctl-session-down	Send a trap when a FortiSwitch controller session goes down.
load-balance-real-server-down	Send a trap when a server load balance real server goes down.
device-new	Send a trap when a new device is found.
per-cpu-high	Send a trap when per-CPU usage is high.

config hosts

Parameter	Description	Type	Size
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified
ip	IPv4 address of the SNMP manager (host).	user	Not Specified
ha-direct	Enable/disable direct management of HA cluster members.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-
	Option **Description** *any* Accept queries from and send traps to this SNMP manager. *query* Accept queries from this SNMP manager but do not send traps. *trap* Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.		

config hosts6

Parameter	Description	Type	Size
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified
ha-direct	Enable/disable direct management of HA cluster members.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-
	Option **Description** *any* Accept queries from and send traps to this SNMP manager. *query* Accept queries from this SNMP manager but do not send traps. *trap* 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
status	Enable/disable this SNMP user.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
trap-status	Enable/disable traps for this SNMP user.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
trap-lport	SNMPv3 local trap port .	integer	Minimum value: 0 Maximum value: 65535
trap-rport	SNMPv3 trap remote port .	integer	Minimum value: 0 Maximum value: 65535
queries	Enable/disable SNMP queries for this user.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
query-port	SNMPv3 query port .	integer	Minimum value: 0 Maximum value: 65535
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
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified
ha-direct	Enable/disable direct management of HA cluster members.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
events	SNMP notifications (traps) to send.	option	-
	Option **Description** *cpu-high* Send a trap when CPU usage is high. *mem-low* Send a trap when available memory is low. *log-full* Send a trap when log disk space becomes low. *intf-ip* Send a trap when an interface IP address is changed. *vpn-tun-up* Send a trap when a VPN tunnel comes up. *vpn-tun-down* Send a trap when a VPN tunnel goes down. *ha-switch* Send a trap after an HA failover when the backup unit has taken over. *ha-hb-failure* Send a trap when HA heartbeats are not received. *ips-signature* Send a trap when IPS detects an attack. *ips-anomaly* Send a trap when IPS finds an anomaly. *av-virus* Send a trap when AntiVirus finds a virus. *av-oversize* Send a trap when AntiVirus finds an oversized file.		

Parameter	Description	Type	Size

Option	Description
av-pattern	Send a trap when AntiVirus finds file matching pattern.
av-fragmented	Send a trap when AntiVirus finds a fragmented file.
fm-if-change	Send a trap when FortiManager interface changes. Send a FortiManager trap.
fm-conf-change	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
bgp-established	Send a trap when a BGP FSM transitions to the established state.
bgp-backward-transition	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
ha-member-up	Send a trap when an HA cluster member goes up.
ha-member-down	Send a trap when an HA cluster member goes down.
ent-conf-change	Send a trap when an entity MIB change occurs (RFC4133).
av-conserve	Send a trap when the FortiGate enters conserve mode.
av-bypass	Send a trap when the FortiGate enters bypass mode.
av-oversize-passed	Send a trap when AntiVirus passes an oversized file.
av-oversize-blocked	Send a trap when AntiVirus blocks an oversized file.
ips-pkg-update	Send a trap when the IPS signature database or engine is updated.
ips-fail-open	Send a trap when the IPS network buffer is full.
faz-disconnect	Send a trap when a FortiAnalyzer disconnects from the FortiGate.
wc-ap-up	Send a trap when a managed FortiAP comes up.
wc-ap-down	Send a trap when a managed FortiAP goes down.
fswctl-session-up	Send a trap when a FortiSwitch controller session comes up.
fswctl-session-down	Send a trap when a FortiSwitch controller session goes down.
load-balance-real-server-down	Send a trap when a server load balance real server goes down.
device-new	Send a trap when a new device is found.
per-cpu-high	Send a trap when per-CPU usage is high.

Parameter	Description	Type	Size
security-level	Security level for message authentication and encryption.	option	-

Option	Description
no-auth-no-priv	Message with no authentication and no privacy (encryption).
auth-no-priv	Message with authentication but no privacy (encryption).
auth-priv	Message with authentication and privacy (encryption).

Parameter	Description	Type	Size
auth-proto	Authentication protocol.	option	-

Option	Description
md5	HMAC-MD5-96 authentication protocol.
sha	HMAC-SHA-96 authentication protocol.
sha224	HMAC-SHA224 authentication protocol.
sha256	HMAC-SHA256 authentication protocol.
sha384	HMAC-SHA384 authentication protocol.
sha512	HMAC-SHA512 authentication protocol.

Parameter	Description	Type	Size
auth-pwd	Password for authentication protocol.	password	Not Specified
priv-proto	Privacy (encryption) protocol.	option	-

Option	Description
aes	CFB128-AES-128 symmetric encryption protocol.
des	CBC-DES symmetric encryption protocol.
aes256	CFB128-AES-256 symmetric encryption protocol.
aes256cisco	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.

Parameter	Description	Type	Size
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified

config system autoupdate push-update

Configure push updates.

```
config system autoupdate push-update
   Description: Configure push updates.
   set status [enable|disable]
   set override [enable|disable]
   set address {string}
   set port {integer}
end
```

config system autoupdate push-update

Parameter	Description	Type	Size
status	Enable/disable push updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
override	Enable/disable push update override server.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
address	IPv4 or IPv6 address used by FortiGuard servers to send push updates to this FortiGate.	string	Maximum length: 63
port	Push update override port. (Do not overlap with other service ports)	integer	Minimum value: 0 Maximum value: 65535

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
status	Enable/disable scheduled updates.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
frequency	Update frequency.	option	-

Option	Description
every	Time interval.
daily	Every day.
weekly	Every week.

Parameter	Description	Type	Size
time	Update time.	user	Not Specified
day	Update day.	option	-

Option	Description
Sunday	Update every Sunday.
Monday	Update every Monday.
Tuesday	Update every Tuesday.
Wednesday	Update every Wednesday.
Thursday	Update every Thursday.
Friday	Update every Friday.
Saturday	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
status	Enable/disable web proxy tunnelling.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
address	Web proxy IP address or FQDN.	string	Maximum length: 63
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535
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 timeout.	user	Not Specified

config port

Parameter	Description	Type	Size
protocol	Protocol .	integer	Minimum value: 0 Maximum value: 255
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535
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|usrgrp]
      set conflicted-ip-timeout {integer}
      set ipsec-lease-hold {integer}
      set auto-configuration [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
status	Enable/disable this DHCP configuration.	option	-

Option	Description
disable	Do not use this DHCP server configuration.
enable	Use this DHCP server configuration.

Parameter	Description	Type	Size
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000
mac-acl-default-action	MAC access control default action (allow or block assigning IP settings).	option	-

Option	Description
assign	Allow the DHCP server to assign IP settings to clients on the MAC access control list.
block	Block the DHCP server from assigning IP settings to clients on the MAC access control list.

Parameter	Description	Type	Size
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-

Option	Description
disable	Disable FortiClient On-Net Status.
enable	Enable FortiClient On-Net Status.

Parameter	Description	Type	Size
dns-service	Options for assigning DNS servers to DHCP clients.	option	-

Option	Description
local	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.
default	Clients are assigned the FortiGate's configured DNS servers.
specify	Specify up to 3 DNS servers in the DHCP server configuration.

Parameter	Description	Type	Size
dns-server1	DNS server 1.	ipv4-address	Not Specified
dns-server2	DNS server 2.	ipv4-address	Not Specified
dns-server3	DNS server 3.	ipv4-address	Not Specified
dns-server4	DNS server 4.	ipv4-address	Not Specified

Parameter	Description	Type	Size
wifi-ac-service	Options for assigning WiFi Access Controllers to DHCP clients	option	-

Option	Description
specify	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.
local	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
wifi-ac2	WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified
wifi-ac3	WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-

Option	Description
local	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.
default	Clients are assigned the FortiGate's configured NTP servers.
specify	Specify up to 3 NTP servers in the DHCP server configuration.

ntp-server1	NTP server 1.	ipv4-address	Not Specified
ntp-server2	NTP server 2.	ipv4-address	Not Specified
ntp-server3	NTP server 3.	ipv4-address	Not Specified
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35
wins-server1	WINS server 1.	ipv4-address	Not Specified
wins-server2	WINS server 2.	ipv4-address	Not Specified
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified
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
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15

Parameter	Description	Type	Size
timezone-option	Options for the DHCP server to set the client's time zone.	option	-

Option	Description
disable	Do not set the client's time zone.
default	Clients are assigned the FortiGate's configured time zone.
specify	Specify the time zone to be assigned to DHCP clients.

timezone	Select the time zone to be assigned to DHCP clients.	option	-

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

Parameter	Description	Type	Size

Option	Description
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
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

Parameter	Description	Type	Size

Option	Description
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 Jayawardenepara
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

Parameter	Description	Type	Size
	Option / **Description** *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	-
	Option / **Description** *regular* Regular DHCP service. *ipsec* DHCP over IPsec service.		
ip-mode	Method used to assign client IP.	option	-
	Option / **Description** *range* Use range defined by start-ip/end-ip to assign client IP. *usrgrp* 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

Parameter	Description	Type	Size
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
auto-configuration	Enable/disable auto configuration.	option	-

Option	Description
disable	Disable auto configuration.
enable	Enable auto configuration.

ddns-update	Enable/disable DDNS update for DHCP.	option	-

Option	Description
disable	Disable DDNS update for DHCP.
enable	Enable DDNS update for DHCP.

ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-

Option	Description
disable	Disable DDNS update override for DHCP.
enable	Enable DDNS update override for DHCP.

ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64
ddns-auth	DDNS authentication mode.	option	-

Option	Description
disable	Disable DDNS authentication.
tsig	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

Parameter	Description	Type	Size
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-

Option	Description
disable	Disable VCI matching.
enable	Enable VCI matching.

Parameter	Description	Type	Size
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
start-ip	Start of IP range.	ipv4-address	Not Specified
end-ip	End of IP range.	ipv4-address	Not Specified

config options

Parameter	Description	Type	Size
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255
type	DHCP option type.	option	-

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.

Parameter	Description	Type	Size
value	DHCP option value.	string	Maximum length: 312
ip	DHCP option IPs.	user	Not Specified

config exclude-range

Parameter	Description	Type	Size
start-ip	Start of IP range.	ipv4-address	Not Specified
end-ip	End of IP range.	ipv4-address	Not Specified

config reserved-address

Parameter	Description	Type	Size
type	DHCP reserved-address type.	option	-

Option	Description
mac	Match with MAC address.
option82	Match with DHCP option 82.

Parameter	Description	Type	Size
ip	IP address to be reserved for the MAC address.	ipv4-address	Not Specified
mac	MAC address of the client that will get the reserved IP address.	mac-address	Not Specified
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-

Option	Description
assign	Configure the client with this MAC address like any other client.
block	Block the DHCP server from assigning IP settings to the client with this MAC address.
reserved	Assign the reserved IP address to the client with this MAC address.

Parameter	Description	Type	Size
circuit-id-type	DHCP option type.	option	-

Option	Description
hex	DHCP option in hex.
string	DHCP option in string.

Parameter	Description	Type	Size
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	-

Option	Description
hex	DHCP option in hex.
string	DHCP option in string.

Parameter	Description	Type	Size
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]
      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
status	Enable/disable this DHCPv6 configuration.	option	-

Option	Description
disable	Enable this DHCPv6 server configuration.
enable	Disable this DHCPv6 server configuration.

Parameter	Description	Type	Size
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-

Option	Description
disable	Do not allow rapid commit.
enable	Allow rapid commit.

Parameter	Description	Type	Size
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-

Option	Description
delegated	Delegated DNS settings.
default	Clients are assigned the FortiGate's configured DNS servers.
specify	Specify up to 3 DNS servers in the DHCPv6 server configuration.

Parameter	Description	Type	Size
dns-search-list	DNS search list options.	option	-

Option	Description
delegated	Delegated the DNS search list.
specify	Specify the DNS search list.

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15
option1	Option 1.	user	Not Specified
option2	Option 2.	user	Not Specified
option3	Option 3.	user	Not Specified
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15
ip-mode	Method used to assign client IP.	option	-

Option	Description
range	Use range defined by start IP/end IP to assign client IP.
delegated	Use delegated prefix method to assign client IP.

config prefix-range

Parameter	Description	Type	Size
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

config ip-range

Parameter	Description	Type	Size
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 80E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61E. 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
status	Enable/disable Modem support (equivalent to bringing an interface up or down).	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* 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	-
	Option **Description** *standalone* Standalone. *redundant* Redundant for an interface.		
auto-dial	Enable/disable auto-dial after a reboot or disconnection.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
dial-on-demand	Enable/disable to dial the modem when packets are routed to the modem interface.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
idle-timer	MODEM connection idle time .	integer	Minimum value: 1 Maximum value: 9999
redial	Redial limit .	option	-
	Option **Description** *none* Forever.		

Parameter	Description	Type	Size
	Option / **Description** *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
holddown-timer	Hold down timer in seconds .	integer	Minimum value: 1 Maximum value: 60
connect-timeout	Connection completion timeout .	integer	Minimum value: 30 Maximum value: 255
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
dont-send-CR1	Do not send CR when connected (ISP1).	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		

Parameter	Description	Type	Size
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	-

Option	Description
generic	All other modem type.
actiontec	ActionTec modem.
ascend_TNT	Ascend TNT modem.

ppp-echo-request1	Enable/disable PPP echo-request to ISP 1.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

authtype1	Allowed authentication types for ISP 1.	option	-

Option	Description
pap	PAP
chap	CHAP
mschap	MSCHAP
mschapv2	MSCHAPv2

dont-send-CR2	Do not send CR when connected (ISP2).	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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	-

Option	Description
generic	All other modem type.
actiontec	ActionTec modem.
ascend_TNT	Ascend TNT modem.

ppp-echo-request2	Enable/disable PPP echo-request to ISP 2.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

authtype2	Allowed authentication types for ISP 2.	option	-

Option	Description
pap	PAP
chap	CHAP
mschap	MSCHAP
mschapv2	MSCHAPv2

dont-send-CR3	Do not send CR when connected (ISP3).	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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	-

Option	Description
generic	All other modem type.
actiontec	ActionTec modem.
ascend_TNT	Ascend TNT modem.

ppp-echo-request3	Enable/disable PPP echo-request to ISP 3.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

altmode	Enable/disable altmode for installations using PPP in China.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

authtype3	Allowed authentication types for ISP 3.	option	-

Option	Description
pap	PAP
chap	CHAP
mschap	MSCHAP
mschapv2	MSCHAPv2

Parameter	Description	Type	Size
traffic-check	Enable/disable traffic-check.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
action	Dial up/stop MODEM.	option	-

Option	Description
dial	Dial up number.
stop	Stop dialup.
none	No action.

Parameter	Description	Type	Size
distance	Distance of learned routes .	integer	Minimum value: 1 Maximum value: 255
priority	Priority of learned routes .	integer	Minimum value: 0 Maximum value: 4294967295

config system 3g-modem custom

This command is available for reference model(s) FortiGate 80E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61E. 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
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
<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
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}
   next
end
```

config system auto-script

Parameter	Description	Type	Size
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535
start	Script starting mode.	option	-
	Option / **Description** *manual* — Starting manually. *auto* — Starting automatically.		
script	List of FortiOS CLI commands to repeat.	var-string	Maximum length: 255
output-size	Number of megabytes to limit script output to .	integer	Minimum value: 10 Maximum value: 1024

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
status	Enable/disable FGFM tunnel.	option	-

Option	Description
enable	Enable management tunnel.
disable	Disable management tunnel.

Parameter	Description	Type	Size
allow-config-restore	Enable/disable allow config restore.	option	-

Option	Description
enable	Enable allow config restore.
disable	Disable allow config restore.

Parameter	Description	Type	Size
allow-push-configuration	Enable/disable push configuration.	option	-

Option	Description
enable	Enable push configuration.
disable	Disable push configuration.

Parameter	Description	Type	Size
allow-push-firmware	Enable/disable push firmware.	option	-

Option	Description
enable	Enable push firmware.
disable	Disable push firmware.

Parameter	Description	Type	Size
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable collection of run time statistics. *disable* / Disable collection of run time statistics.		
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-
	Option / **Description** *enable* / Enable restriction of authorized manager only. *disable* / 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
ip	IP address.	ipv4-address-any	Not Specified
vdom	Virtual domain name.	string	Maximum length: 31
ipsec	Enable/disable FortiManager IPsec tunnel.	option	-
	Option / **Description** *enable* / Enable FortiManager IPsec tunnel. *disable* / Disable FortiManager IPsec tunnel.		

Parameter	Description	Type	Size
central-management	Enable/disable FortiManager central management.	option	-

Option	Description
enable	Enable central management.
disable	Disable central management.

Parameter	Description	Type	Size
central-mgmt-auto-backup	Enable/disable central management auto backup.	option	-

Option	Description
enable	Enable auto backup.
disable	Disable auto backup.

Parameter	Description	Type	Size
central-mgmt-schedule-config-restore	Enable/disable central management schedule config restore.	option	-

Option	Description
enable	Enable central management scheduled restore.
disable	Disable central management scheduled restore.

Parameter	Description	Type	Size
central-mgmt-schedule-script-restore	Enable/disable central management schedule script restore.	option	-

Option	Description
enable	Enable central management scheduled restore.
disable	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
status	Enable/disable FM.	option	-
	Option / **Description** *enable* — Enable FM. *disable* — Disable FM.		
id	ID.	string	Maximum length: 35
ip	IP address.	ipv4-address	Not Specified
vdom	VDOM.	string	Maximum length: 31
auto-backup	Enable/disable automatic backup.	option	-
	Option / **Description** *enable* — Enable automatic backup. *disable* — Disable automatic backup.		
scheduled-config-restore	Enable/disable scheduled configuration restore.	option	-
	Option / **Description** *enable* — Enable scheduled configuration restore. *disable* — Disable scheduled configuration restore.		
ipsec	Enable/disable IPsec.	option	-
	Option / **Description** *enable* — Enable IPsec. *disable* — 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 severs 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
mode	Central management mode.	option	-

Option	Description
normal	Manage and configure this FortiGate from FortiManager.
backup	Manage and configure this FortiGate locally and back up its configuration to FortiManager.

Parameter	Description	Type	Size
type	Central management type.	option	-

Option	Description
fortimanager	FortiManager.
fortiguard	Central management of this FortiGate using FortiCloud.
none	No central management.

Parameter	Description	Type	Size
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiGate.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable scheduled configuration restore. *disable* Disable scheduled configuration restore.		
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiGate.	option	-
	Option **Description** *enable* Enable scheduled script restore. *disable* Disable scheduled script restore.		
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiGate.	option	-
	Option **Description** *enable* Enable push configuration. *disable* Disable push configuration.		
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiGate.	option	-
	Option **Description** *enable* Enable push firmware. *disable* Disable push firmware.		
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiGate from the central management server.	option	-
	Option **Description** *enable* Enable remote firmware upgrade. *disable* Disable remote firmware upgrade.		
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiGate	option	-
	Option **Description** *enable* Enable remote monitoring of device. *disable* Disable remote monitoring of device.		

Parameter	Description	Type	Size
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
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
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-

Option	Description
8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.
443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.

include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-

Option	Description
enable	Enable inclusion of public FortiGuard servers in the override server list.
disable	Disable inclusion of public FortiGuard servers in the override server list.

enc-algorithm	Encryption strength for communications between the FortiGate and central management.	option	-

Option	Description
default	High strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD.
high	128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA.
low	64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CDBC-SHA, DES-CBC-SHA, DES-CBC-MD5.

Parameter	Description	Type	Size
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

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 server-list

Parameter	Description	Type	Size
server-type	FortiGuard service type.	option	-

Option	Description
update	AV, IPS, and AV-query update server.
rating	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	-

Option	Description
ipv4	IPv4 address.
ipv6	IPv6 address.
fqdn	FQDN.

server-address	IPv4 address of override server.	ipv4-address	Not Specified
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
description	Description.	string	Maximum length: 127
intrazone	Allow or deny traffic routing between different interfaces in the same zone .	option	-
	Option / **Description** *allow* — Allow traffic between interfaces in the zone. *deny* — 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
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
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 ha-status [disable|enable]
      set server {string}
      set server-port {integer}
      set username {string}
      set password {password_aes256}
      set access-key {string}
      set secret-key {password}
      set region {string}
      set vpc-id {string}
      set tenant-id {string}
      set subscription-id {string}
      set login-endpoint {string}
      set resource-url {string}
      set client-id {string}
      set client-secret {password}
      set resource-group {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 use-metadata-iam [disable|enable]
      set gcp-project {string}
      set service-account {string}
      set private-key {user}
      set secret-token {user}
      set domain {string}
      set group-name {string}
      set update-interval {integer}
   next
end
```

config system sdn-connector

Parameter	Description	Type	Size
status	Enable/disable connection to the remote SDN connector.	option	-

Option	Description
disable	Disable connection to this SDN Connector.
enable	Enable connection to this SDN Connector.

type	Type of SDN connector.	option	-

Parameter	Description	Type	Size
	Option / **Description** *aci* — Application Centric Infrastructure (ACI). *alicloud* — AliCloud Service (ACS). *aws* — Amazon Web Services (AWS). *azure* — Microsoft Azure. *gcp* — Google Cloud Platform (GCP). *nsx* — VMware NSX. *nuage* — Nuage VSP. *oci* — Oracle Cloud Infrastructure. *openstack* — OpenStack. *kubernetes* — Kubernetes. *vmware* — VMware vSphere (vCenter & ESXi). *sepm* — Symantec Endpoint Protection Manager.		
ha-status	Enable/disable use for FortiGate HA service.	option	-
	Option / **Description** *disable* — Disable use for FortiGate HA service. *enable* — Enable use for FortiGate HA service.		
server	Server address of the remote SDN connector.	string	Maximum length: 127
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified
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

Parameter	Description	Type	Size
vpc-id	AWS VPC ID.	string	Maximum length: 31
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127
subscription-id	Azure subscription ID.	string	Maximum length: 63
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127
resource-url	Azure Stack resource URL.	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
resource-group	Azure resource group.	string	Maximum length: 63
azure-region	Azure server region.	option	-

Option	Description
global	Global Azure Server.
china	China Azure Server.
germany	Germany Azure Server.
usgov	US Government Azure Server.
local	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	-

Option	Description
commercial	Commercial region.
government	Government region.

Parameter	Description	Type	Size
oci-cert	OCI certificate.	string	Maximum length: 63
oci-fingerprint	OCI pubkey fingerprint.	string	Maximum length: 63
use-metadata-iam	Enable/disable using IAM role from metadata to call API.	option	-

Option	Description
disable	Disable using IAM role to call API.
enable	Enable using IAM role to call API.

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
update-interval	Dynamic object update interval .	integer	Minimum value: 0 Maximum value: 3600

config ip

Parameter	Description	Type	Size
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
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63

Parameter	Description	Type	Size
resource-group	Resource group of Azure route table.	string	Maximum length: 63

config route

Parameter	Description	Type	Size
next-hop	Next hop address.	string	Maximum length: 127

config route

Parameter	Description	Type	Size
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 auto-asic-offload [enable|disable]
   next
end
```

config system ipv6-tunnel

Parameter	Description	Type	Size
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
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-

Parameter	Description	Type	Size

Option	Description
enable	Enable auto ASIC offloading.
disable	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 status [enable|disable]
      set type [category|address|...]
      set category {integer}
      set username {string}
      set password {password}
      set comments {var-string}
      set resource {string}
      set refresh-rate {integer}
      set source-ip {ipv4-address}
   next
end
```

config system external-resource

Parameter	Description	Type	Size
status	Enable/disable user resource.	option	-

Option	Description
enable	Enable user resource.
disable	Disable user resource.

Parameter	Description	Type	Size
type	User resource type.	option	-

Option	Description
category	FortiGuard category.
address	Firewall IP address.
domain	Domain Name.
malware	Malware hash.

Parameter	Description	Type	Size
category	User resource category.	integer	Minimum value: 192 Maximum value: 221
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
refresh-rate	Time interval to refresh external resource .	integer	Minimum value: 1 Maximum value: 43200
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified

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
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-

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	-

Parameter	Description	Type	Size

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
status	Enable/disable this server for IPv6 DNS queries.	option	-

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
destination-visibility	Enable/disable logging of destination visibility.	option	-

Option	Description
disable	Disable logging of destination visibility.
enable	Enable logging of destination visibility.

Parameter	Description	Type	Size
source-location	Enable/disable logging of source geographical location visibility.	option	-

Option	Description
disable	Disable logging of source geographical location visibility.
enable	Enable logging of source geographical location visibility.

Parameter	Description	Type	Size
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-

Option	Description
disable	Disable logging of destination hostname visibility.
enable	Enable logging of destination hostname visibility.

Parameter	Description	Type	Size
hostname-ttl	TTL of hostname table entries .	integer	Minimum value: 60 Maximum value: 86400
hostname-limit	Limit of the number of hostname table entries .	integer	Minimum value: 0 Maximum value: 50000
destination-location	Enable/disable logging of destination geographical location visibility.	option	-

Option	Description
disable	Disable logging of destination geographical location visibility.
enable	Enable logging of destination geographical location visibility.

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 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
interface	Interface name.	string	Maximum length: 15
ip-version	IP version to use for VPN interface.	option	-

Option	Description
4	Use IPv4 addressing for gateways.
6	Use IPv6 addressing for gateways.

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
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified
dscp-copying	Enable/disable DSCP copying.	option	-

Option	Description
disable	Disable DSCP copying.
enable	Enable DSCP copying.

diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified

Parameter	Description	Type	Size
keepalive-interval	Keepalive message interval .	integer	Minimum value: 0 Maximum value: 32767
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down .	integer	Minimum value: 1 Maximum value: 255

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
member <tunnel-name>	Member tunnels of the aggregate. Tunnel name.	string	Maximum length: 79
algorithm	Frame distribution algorithm.	option	-

Option	Description
L3	Use layer 3 address for distribution.
L4	Use layer 4 information for distribution.
round-robin	Per-packet round-robin distribution.
redundant	Use first tunnel that is up for all traffic.

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 auto-asic-offload [enable|disable]
   next
end
```

config system ipip-tunnel

Parameter	Description	Type	Size
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
local-gw	IPv4 address for the local gateway.	ipv4-address-any	Not Specified
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-

Option	Description
enable	Enable auto ASIC offloading.
disable	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
status	Enable/disable this mobile tunnel.	option	-
	Option **Description** *disable* Disable this mobile tunnel. *enable* 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
home-address	Home IP address (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
renew-interval	Time before lifetime expiraton to send NMMO HA re-registration .	integer	Minimum value: 5 Maximum value: 60
lifetime	NMMO HA registration request lifetime .	integer	Minimum value: 180 Maximum value: 65535
reg-interval	NMMO HA registration interval .	integer	Minimum value: 5 Maximum value: 300
reg-retry	Maximum number of NMMO HA registration retries .	integer	Minimum value: 1 Maximum value: 30
n-mhae-spi	NEMO authentication SPI .	integer	Minimum value: 0 Maximum value: 4294967295
n-mhae-key-type	NEMO authentication key type (ascii or base64).	option	-

Parameter	Description	Type	Size
	Option **Description** *ascii* The authentication key is an ASCII string. *base64* The authentication key is Base64 encoded.		
n-mhae-key	NEMO authentication key.	user	Not Specified
hash-algorithm	Hash Algorithm (Keyed MD5).	option	-
	Option **Description** *hmac-md5* Keyed MD5.		
tunnel-mode	NEMO tunnnel mode (GRE tunnel).	option	-
	Option **Description** *gre* GRE tunnel.		

config network

Parameter	Description	Type	Size
interface	Select the associated interface name from available options.	string	Maximum length: 15
prefix	Class IP and Netmask with correction (Format:xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/x).	ipv4-classnet	Not Specified

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
dial-on-demand	Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE interface.	option	-

Option	Description
enable	Enable dial on demand.
disable	Disable dial on demand.

Parameter	Description	Type	Size
ipv6	Enable/disable IPv6 Control Protocol (IPv6CP).	option	-

Option	Description
enable	Enable IPv6CP.
disable	Disable IPv6CP.

Parameter	Description	Type	Size
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	-

Option	Description
auto	Automatically choose the authentication method.
pap	PAP authentication.
chap	CHAP authentication.
mschapv1	MS-CHAPv1 authentication.
mschapv2	MS-CHAPv2 authentication.

Parameter	Description	Type	Size
ipunnumbered	PPPoE unnumbered IP.	ipv4-address	Not Specified
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable PPPoE unnumbered negotiation. *disable* / Disable PPPoE unnumbered negotiation.		
idle-timeout	PPPoE auto disconnect after idle timeout .	integer	Minimum value: 0 Maximum value: 4294967295
disc-retry-timeout	PPPoE discovery init timeout value in .	integer	Minimum value: 0 Maximum value: 4294967295
padt-retry-timeout	PPPoE terminate timeout value in .	integer	Minimum value: 0 Maximum value: 4294967295
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
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767

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
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast or multicast.	option	-

Option	Description
ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.
ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.
ipv4-multicast	Use IPv4 multicast addressing over the VXLAN.
ipv6-multicast	Use IPv6 multicast addressing over the VXLAN.

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
multicast-ttl	VXLAN multicast TTL .	integer	Minimum value: 1 Maximum value: 255

config system geneve

Configure GENEVE devices.

```
config system geneve
   Description: Configure GENEVE devices.
   edit <name>
      set interface {string}
      set vni {integer}
      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
interface	Outgoing interface for GENEVE encapsulated traffic.	string	Maximum length: 15
vni	GENEVE network ID.	integer	Minimum value: 0 Maximum value: 16777215
ip-version	IP version to use for the GENEVE interface and so for communication over the GENEVE. IPv4 or IPv6 unicast.	option	-
	Option / **Description** *ipv4-unicast* — Use IPv4 unicast addressing over the GENEVE. *ipv6-unicast* — 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
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

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
member <interface-name>	Interfaces belong to the virtual-wire-pair. Interface name.	string	Maximum length: 79
wildcard-vlan	Enable/disable wildcard VLAN.	option	-
	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 [master|slave]
      set view [shadow|public]
      set ip-master {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}
      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
status	Enable/disable this DNS zone.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
domain	Domain name.	string	Maximum length: 255
allow-transfer	DNS zone transfer IP address list.	user	Not Specified
type	Zone type (master to manage entries directly, slave to import entries from other zones).	option	-
	Option / **Description** *master* / Master DNS zone, to manage entries directly. *slave* / Slave DNS zone, to import entries from other DNS zones.		
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-
	Option / **Description** *shadow* / Shadow DNS zone to serve internal clients. *public* / Public DNS zone to serve public clients.		
ip-master	IP address of master DNS server. Entries in this master DNS server and imported into the DNS zone.	ipv4-address-any	Not Specified
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255
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

Parameter	Description	Type	Size
ttl	Default time-to-live value for the entries of this DNS zone .	integer	Minimum value: 0 Maximum value: 2147483647
authoritative	Enable/disable authoritative zone.	option	-

Option	Description
enable	Enable authoritative zone.
disable	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

config dns-entry

Parameter	Description	Type	Size
status	Enable/disable resource record status.	option	-

Option	Description
enable	Enable resource record status.
disable	Disable resource record status.

type	Resource record type.	option	-

Option	Description
A	Host type.
NS	Name server type.
CNAME	Canonical name type.
MX	Mail exchange type.
AAAA	IPv6 host type.
PTR	Pointer type.
PTR_V6	IPv6 pointer type.

ttl	Time-to-live for this entry .	integer	Minimum value: 0 Maximum value: 2147483647

Parameter	Description	Type	Size
preference	DNS entry preference, 0 is the highest preference	integer	Minimum value: 0 Maximum value: 65535
ip	IPv4 address of the host.	ipv4-address-any	Not Specified
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}
   next
end
```

config system dns-server

Parameter	Description	Type	Size
mode	DNS server mode.	option	-

Option	Description
recursive	Shadow DNS database and forward.
non-recursive	Public DNS database only.
forward-only	Forward only.

Parameter	Description	Type	Size
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35

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
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

Parameter	Description	Type	Size
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 (IPv4, IPv6, policy46, policy64, 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
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

Parameter	Description	Type	Size
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
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295
log-disk-quota	Log disk quota in MB.	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
description	Description.	string	Maximum length: 127
snmp-index	Permanent SNMP Index of the virtual domain .	integer	Minimum value: 0 Maximum value: 4294967295
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 (IPv4, IPv6, policy46, policy64, 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

Parameter	Description	Type	Size
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
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified
log-disk-quota	Log disk quota in MB (range depends on how much disk space is available).	user	Not Specified

config system virtual-wan-link

Configure redundant internet connections using SD-WAN (formerly virtual WAN link).

```
config system virtual-wan-link
   Description: Configure redundant internet connections using SD-WAN (formerly virtual WAN
        link).
   set status [disable|enable]
   set load-balance-mode [source-ip-based|weight-based|...]
   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>
      next
   end
   config members
      Description: FortiGate interfaces added to the virtual-wan-link.
      edit <seq-num>
         set interface {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 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 server {string}
      set protocol [ping|tcp-echo|...]
      set port {integer}
      set security-mode [none|authentication]
      set password {password}
      set packet-size {integer}
      set ha-priority {integer}
      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 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 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 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-id <id1>, <id2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-app-ctrl <id1>, <id2>, ...
        set internet-service-app-ctrl-group <name1>, <name2>, ...
        set health-check {string}
        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 status [enable|disable]
        set gateway [enable|disable]
        set default [enable|disable]
        set sla-compare-method [order|number]
     next
   end
end
```

config system virtual-wan-link

Parameter	Description	Type	Size
status	Enable/disable SD-WAN.	option	-

Option	Description
disable	Disable SD-WAN.
enable	Enable SD-WAN.

Parameter	Description	Type	Size
load-balance-mode	Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.	option	-

Option	Description
source-ip-based	Source IP load balancing. All traffic from a source IP is sent to the same interface.
weight-based	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.
usage-based	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.
source-dest-ip-based	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.
measured-volume-based	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.

Parameter	Description	Type	Size
neighbor-hold-down	Enable/disable hold switching from the secondary neighbor to the primary neighbor.	option	-

Option	Description
enable	Enable hold switching from the secondary neighbor to the primary neighbor.
disable	Disable hold switching from the secondary neighbor to the primary neighbor.

Parameter	Description	Type	Size
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
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

Parameter	Description	Type	Size
fail-detect	Enable/disable SD-WAN Internet connection status checking (failure detection).	option	-

Option	Description
enable	Enable status checking.
disable	Disable status checking.

fail-alert-interfaces <name>	Physical interfaces that will be alerted. Physical interface name.	string	Maximum length: 79

config members

Parameter	Description	Type	Size
interface	Interface name.	string	Maximum length: 15
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
source	Source IP address used in the health-check packet to the server.	ipv4-address	Not Specified
gateway6	IPv6 gateway.	ipv6-address	Not Specified
source6	Source IPv6 address used in the health-check packet to the server.	ipv6-address	Not Specified
cost	Cost of this interface for services in SLA mode .	integer	Minimum value: 0 Maximum value: 4294967295
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
priority	Priority of the interface . Used for SD-WAN rules or priority rules.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
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
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
volume-ratio	Measured volume ratio .	integer	Minimum value: 1 Maximum value: 255
status	Enable/disable this interface in the SD-WAN.	option	-

Option	Description
disable	Disable this interface in the SD-WAN.
enable	Enable this interface in the SD-WAN.

comment	Comments.	var-string	Maximum length: 255

config health-check

Parameter	Description	Type	Size
probe-packets	Enable/disable transmission of probe packets.	option	-

Option	Description
disable	Disable transmission of probe packets.
enable	Enable transmission of probe packets.

addr-mode	Address mode (IPv4 or IPv6).	option	-

Option	Description
ipv4	IPv4 mode.
ipv6	IPv6 mode.

server	IP address or FQDN name of the server.	string	Maximum length: 79

Parameter	Description	Type	Size
protocol	Protocol used to determine if the FortiGate can communicate with the server.	option	-

Option	Description
ping	Use PING to test the link with the server.
tcp-echo	Use TCP echo to test the link with the server.
udp-echo	Use UDP echo to test the link with the server.
http	Use HTTP-GET to test the link with the server.
twamp	Use TWAMP to test the link with the server.
ping6	PING6 link monitor.

port	Port number used to communicate with the server over the selected protocol.	integer	Minimum value: 1 Maximum value: 65535
security-mode	Twamp controller security mode.	option	-

Option	Description
none	Unauthenticated mode.
authentication	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
ha-priority	HA election priority .	integer	Minimum value: 1 Maximum value: 50
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
http-match	Response string expected from the server if the protocol is HTTP.	string	Maximum length: 1024

Parameter	Description	Type	Size
interval	Status check interval in milliseconds, or the time between attempting to connect to the server .	integer	Minimum value: 500 Maximum value: 3600000
probe-timeout	Time to wait before a probe packet is considered lost .	integer	Minimum value: 500 Maximum value: 5000
failtime	Number of failures before server is considered lost .	integer	Minimum value: 1 Maximum value: 3600
recoverytime	Number of successful responses received before server is considered recovered .	integer	Minimum value: 1 Maximum value: 3600
diffservcode	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	-

Option	Description
enable	Enable update cascade interface.
disable	Disable update cascade interface.

update-static-route	Enable/disable updating the static route.	option	-

Option	Description
enable	Enable updating the static route.
disable	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
sla-pass-log-period	Time interval in seconds that SLA pass log messages will be generated .	integer	Minimum value: 0 Maximum value: 3600

Parameter	Description	Type	Size
threshold-warning-packetloss	Warning threshold for packet loss .	integer	Minimum value: 0 Maximum value: 100
threshold-alert-packetloss	Alert threshold for packet loss .	integer	Minimum value: 0 Maximum value: 100
threshold-warning-latency	Warning threshold for latency .	integer	Minimum value: 0 Maximum value: 4294967295
threshold-alert-latency	Alert threshold for latency .	integer	Minimum value: 0 Maximum value: 4294967295
threshold-warning-jitter	Warning threshold for jitter .	integer	Minimum value: 0 Maximum value: 4294967295
threshold-alert-jitter	Alert threshold for jitter .	integer	Minimum value: 0 Maximum value: 4294967295
members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295

config sla

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

config neighbor

Parameter	Description	Type	Size
member	Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295
role	Role of neighbor.	option	-

Option	Description
standalone	Standalone neighbor.
primary	Primary neighbor.
secondary	Secondary neighbor.

health-check	SD-WAN health-check name.	string	Maximum length: 35
sla-id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295

config service

Parameter	Description	Type	Size
name	Priority rule name.	string	Maximum length: 35
addr-mode	Address mode (IPv4 or IPv6).	option	-

Option	Description
ipv4	IPv4 mode.
ipv6	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	-

Option	Description
enable	Enable negation of input device match.
disable	Disable negation of input device match.

Parameter	Description	Type	Size
mode	Control how the priority rule sets the priority of interfaces in the SD-WAN.	option	-

Option	Description
auto	Assign interfaces a priority based on quality.
manual	Assign interfaces a priority manually.
priority	Assign interfaces a priority based on the link-cost-factor quality of the interface.
sla	Assign interfaces a priority based on selected SLA settings.
load-balance	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.

role	Service role to work with neighbor.	option	-

Option	Description
standalone	Standalone service.
primary	Primary service for primary neighbor.
secondary	Secondary service for secondary neighbor.

standalone-action	Enable/disable service when selected neighbor role is standalone while service role is not standalone.	option	-

Option	Description
enable	Enable service when selected neighbor role is standalone.
disable	Disable service when selected neighbor role is standalone.

quality-link	Quality grade.	integer	Minimum value: 0 Maximum value: 255
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

Parameter	Description	Type	Size
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535
route-tag	IPv4 route map route-tag.	integer	Minimum value: 0 Maximum value: 4294967295
dst <name>	Destination address name. Address or address group name.	string	Maximum length: 79
dst-negate	Enable/disable negation of destination address match.	option	-

Option	Description
enable	Enable destination address negation.
disable	Disable destination address negation.

src <name>	Source address name. Address or address group name.	string	Maximum length: 79
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	-

Option	Description
enable	Enable source address negation.
disable	Disable source address negation.

users <name>	User name. User name.	string	Maximum length: 79
groups <name>	User groups. Group name.	string	Maximum length: 79

Parameter	Description	Type	Size
internet-service	Enable/disable use of Internet service for application-based load balancing.	option	-

Option	Description
enable	Enable cloud service to support application-based load balancing.
disable	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-id <id>	Internet service ID list. Internet service ID.	integer	Minimum value: 0 Maximum value: 4294967295
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
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	Health check.	string	Maximum length: 35
link-cost-factor	Link cost factor.	option	-

Option	Description
latency	Select link based on latency.
jitter	Select link based on jitter.
packet-loss	Select link based on packet loss.

Parameter	Description	Type	Size
	Option — **Description** *inbandwidth* — Select link based on available bandwidth of incoming traffic. *outbandwidth* — Select link based on available bandwidth of outgoing traffic. *bibandwidth* — Select link based on available bandwidth of bidirectional traffic. *custom-profile-1* — 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
latency-weight	Coefficient of latency in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
jitter-weight	Coefficient of jitter in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
bandwidth-weight	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
link-cost-threshold	Percentage threshold change of link cost values that will result in policy route regeneration .	integer	Minimum value: 0 Maximum value: 10000000
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
dscp-forward	Enable/disable forward traffic DSCP tag.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable use of forward DSCP tag. *disable* — Disable use of forward DSCP tag.		
dscp-reverse	Enable/disable reverse traffic DSCP tag.	option	-
	Option / **Description** *enable* — Enable use of reverse DSCP tag. *disable* — 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
status	Enable/disable SD-WAN service.	option	-
	Option / **Description** *enable* — Enable virtual WAN link service. *disable* — Disable virtual WAN link service.		
gateway	Enable/disable SD-WAN service gateway.	option	-
	Option / **Description** *enable* — Enable SD-WAN service gateway. *disable* — Disable SD-WAN service gateway.		
default	Enable/disable use of SD-WAN as default service.	option	-
	Option / **Description** *enable* — Enable use of SD-WAN as default service. *disable* — Disable use of SD-WAN as default service.		
sla-compare-method	Method to compare SLA value for sla and load balance mode.	option	-

Parameter	Description	Type	Size
	Option — **Description** *order* — Compare SLA value based on the order of health-check. *number* — Compare SLA value based on the number of satisfied health-check. Limits health-checks to only configured member interfaces.		

config sla

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

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
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295

config host

Parameter	Description	Type	Size
ip	Server host IPv4 address.	ipv4-address	Not Specified
port	Server host port number to communicate with client.	integer	Minimum value: 1 Maximum value: 65535
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
comment	Comment.	var-string	Maximum length: 1023

config voice

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

Option	Description
disable	Disable advertising this LLDP network policy.

Parameter	Description	Type	Size
	Option **Description** *enable* Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-
	Option **Description** *none* Advertise that untagged frames should be used. *dot1q* Advertise that 802.1Q (VLAN) tagging should be used. *dot1p* Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config voice-signaling

Parameter	Description	Type	Size
status	Enable/disable advertising this policy.	option	-
	Option **Description** *disable* Disable advertising this LLDP network policy. *enable* Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-
	Option **Description** *none* Advertise that untagged frames should be used. *dot1q* Advertise that 802.1Q (VLAN) tagging should be used. *dot1p* Advertise that 802.1P priority tagging (VLAN 0) should be used.		

Parameter	Description	Type	Size
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config guest

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

Option	Description
disable	Disable advertising this LLDP network policy.
enable	Enable advertising this LLDP network policy.

Parameter	Description	Type	Size
tag	Advertise tagged or untagged traffic.	option	-

Option	Description
none	Advertise that untagged frames should be used.
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.

Parameter	Description	Type	Size
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config guest-voice-signaling

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

Option	Description
disable	Disable advertising this LLDP network policy.
enable	Enable advertising this LLDP network policy.

Parameter	Description	Type	Size
tag	Advertise tagged or untagged traffic.	option	-

Option	Description
none	Advertise that untagged frames should be used.
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.

Parameter	Description	Type	Size
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config softphone

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

Option	Description
disable	Disable advertising this LLDP network policy.
enable	Enable advertising this LLDP network policy.

Parameter	Description	Type	Size
tag	Advertise tagged or untagged traffic.	option	-

Parameter	Description	Type	Size
	Option **Description** *none* Advertise that untagged frames should be used. *dot1q* Advertise that 802.1Q (VLAN) tagging should be used. *dot1p* Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config video-conferencing

Parameter	Description	Type	Size
status	Enable/disable advertising this policy.	option	-
	Option **Description** *disable* Disable advertising this LLDP network policy. *enable* Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-
	Option **Description** *none* Advertise that untagged frames should be used. *dot1q* Advertise that 802.1Q (VLAN) tagging should be used. *dot1p* Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094

Parameter	Description	Type	Size
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config streaming-video

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

Option	Description
disable	Disable advertising this LLDP network policy.
enable	Enable advertising this LLDP network policy.

tag	Advertise tagged or untagged traffic.	option	-

Option	Description
none	Advertise that untagged frames should be used.
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.

vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

config video-signaling

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

Option	Description
disable	Disable advertising this LLDP network policy.
enable	Enable advertising this LLDP network policy.

Parameter	Description	Type	Size
tag	Advertise tagged or untagged traffic.	option	-

Option	Description
none	Advertise that untagged frames should be used.
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.

Parameter	Description	Type	Size
vlan	802.1Q VLAN ID to advertise .	integer	Minimum value: 1 Maximum value: 4094
priority	802.1P CoS/PCP to advertise .	integer	Minimum value: 0 Maximum value: 7
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

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 slave-add-ike-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
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
peerip	IP address of the interface on the peer unit that is used for the session synchronization link.	ipv4-address	Not Specified
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
hb-lost-threshold	Lost heartbeat threshold .	integer	Minimum value: 1 Maximum value: 10
ipsec-tunnel-sync	Enable/disable IPsec tunnel synchronization.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable IPsec tunnel synchronization. *disable* — Disable IPsec tunnel synchronization.		
slave-add-ike-routes	Enable/disable IKE route announcement on the backup unit.	option	-
	Option / **Description** *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
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
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
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
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

config custom-service

Parameter	Description	Type	Size
src-port-range	Custom service source port range.	user	Not Specified
dst-port-range	Custom service destination port range.	user	Not Specified

config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
   Description: Configure FortiGuard services.
   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 fortiguard-anycast [enable|disable]
   set fortiguard-anycast-source [fortinet|aws|...]
   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 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 ddns-server-ip {ipv4-address}
   set ddns-server-port {integer}
   set interface-select-method [auto|sdwan|...]
   set interface {string}
end
```

config system fortiguard

Parameter	Description	Type	Size
protocol	Protocol used to communicate with the FortiGuard servers.	option	-

Option	Description
udp	UDP for server communication (for use by FortiGuard or FortiManager).
http	HTTP for server communication (for use only by FortiManager).
https	HTTPS for server communication (for use by FortiGuard or FortiManager).

Parameter	Description	Type	Size
port	Port used to communicate with the FortiGuard servers.	option	-

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.

Parameter	Description	Type	Size
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266
auto-join-forticloud *	Automatically connect to and login to FortiCloud.	option	-

Option	Description
enable	Enable automatic connection and login to FortiCloud.
disable	Disable automatic connection and login to FortiCloud.

Parameter	Description	Type	Size
update-server-location	Signature update server location.	option	-

Option	Description
usa	FGD servers in United States.
any	FGD servers in any location.

Parameter	Description	Type	Size
sandbox-region	Cloud sandbox region.	string	Maximum length: 63
fortiguard-anycast	Enable/disable use of FortiGuard's anycast network.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable use of FortiGuard's anycast network. *disable* — 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	-
	Option / **Description** *fortinet* — Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. *aws* — Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network. *debug* — Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.		
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-
	Option / **Description** *enable* — Turn off the FortiGuard antispam service. *disable* — Allow the FortiGuard antispam service.		
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-
	Option / **Description** *enable* — Enable FortiGuard antispam request caching. *disable* — Disable FortiGuard antispam request caching.		
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
antispam-cache-mpercent	Maximum percent of FortiGate memory the antispam cache is allowed to use .	integer	Minimum value: 1 Maximum value: 15

Parameter	Description	Type	Size
antispam-license	Interval of time between license checks for the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295
antispam-expiration	Expiration date of the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295
antispam-timeout	Antispam query time out .	integer	Minimum value: 1 Maximum value: 30
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-

Option	Description
enable	Turn off FortiGuard antivirus service.
disable	Allow the FortiGuard antivirus service.

Parameter	Description	Type	Size
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-

Option	Description
enable	Enable FortiGuard antivirus caching.
disable	Disable FortiGuard antivirus caching.

Parameter	Description	Type	Size
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries .	integer	Minimum value: 300 Maximum value: 86400
outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use .	integer	Minimum value: 1 Maximum value: 15

Parameter	Description	Type	Size
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out .	integer	Minimum value: 1 Maximum value: 30
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-

Option	Description
enable	Turn off the FortiGuard web filtering service.
disable	Allow the FortiGuard web filtering service to operate.

webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-

Option	Description
enable	Enable FortiGuard web filter caching.
disable	Disable FortiGuard web filter caching.

webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds .	integer	Minimum value: 300 Maximum value: 86400
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295
webfilter-expiration	Expiration date of the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
webfilter-timeout	Web filter query time out .	integer	Minimum value: 1 Maximum value: 30
sdns-server-ip	IP address of the FortiDNS server.	user	Not Specified
sdns-server-port	Port used to communicate with FortiDNS servers.	integer	Minimum value: 1 Maximum value: 65535
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified
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
proxy-server-port	Port used to communicate with the proxy server.	integer	Minimum value: 0 Maximum value: 65535
proxy-username	Proxy user name.	string	Maximum length: 64
proxy-password	Proxy user password.	password	Not Specified
ddns-server-ip	IP address of the FortiDDNS server.	ipv4-address	Not Specified
ddns-server-port	Port used to communicate with FortiDDNS servers.	integer	Minimum value: 1 Maximum value: 65535
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

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

* This parameter may not exist in some models.

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|...]
end
```

config system email-server

Parameter	Description	Type	Size
type	Use FortiGuard Message service or custom email server.	option	-
	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

Parameter	Description	Type	Size
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified
authenticate	Enable/disable authentication.	option	-

Option	Description
enable	Enable authentication.
disable	Disable authentication.

Parameter	Description	Type	Size
validate-server	Enable/disable validation of server certificate.	option	-

Option	Description
enable	Enable validation of server certificate.
disable	Disable validation of server certificate.

Parameter	Description	Type	Size
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	-

Option	Description
none	None.
starttls	STARTTLS.
smtps	SSL/TLS.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

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
status	Enable/disable alarm.	option	-

Option	Description
enable	Enable alarm.
disable	Disable alarm.

Parameter	Description	Type	Size
audible	Enable/disable audible alarm.	option	-

Option	Description
enable	Enable audible alarm.
disable	Disable audible alarm.

config groups

Parameter	Description	Type	Size
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024
user-auth-failure-threshold	User authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024
user-auth-lockout-threshold	User authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024
replay-attempt-threshold	Replay attempt threshold.	integer	Minimum value: 0 Maximum value: 1024
self-test-failure-threshold	Self-test failure threshold.	integer	Minimum value: 0 Maximum value: 1
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024

Parameter	Description	Type	Size
decryption-failure-threshold	Decryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024
fw-policy-id	Firewall policy ID.	integer	Minimum value: 0 Maximum value: 4294967295
fw-policy-id-threshold	Firewall policy ID threshold.	integer	Minimum value: 0 Maximum value: 1024

config fw-policy-violations

Parameter	Description	Type	Size
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024
src-ip	Source IP (0=all).	ipv4-address	Not Specified
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535

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
interface	Interface name.	string	Maximum length: 35
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified

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
name	Helper name.	option	-

Option	Description
ftp	FTP.
tftp	TFTP.
ras	RAS.
h323	H323.
tns	TNS.
mms	MMS.
sip	SIP.
pptp	PPTP.
rtsp	RTSP.
dns-udp	DNS UDP.
dns-tcp	DNS TCP.
pmap	PMAP.
rsh	RSH.

Parameter	Description	Type	Size
	Option / **Description** *dcerpc* / DCERPC. *mgcp* / MGCP.		
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535

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
interface	Interface acting proxy-ARP.	string	Maximum length: 15
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified

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
status	Enable/disable FIPS-CC mode.	option	-

Option	Description
enable	Enable/disable FIPS-CC mode.
disable	Disable FIPS-CC mode.

Parameter	Description	Type	Size
entropy-token	Enable/disable/dynamic entropy token.	option	-

Option	Description
enable	Enable entropy token to be present during boot process.
disable	Disable entropy token to be present during boot process.
dynamic	Dynamic detect entropy token to be present during boot process.

Parameter	Description	Type	Size
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440
key-generation-self-test	Enable/disable self tests after key generation.	option	-

Option	Description
enable	Enable self tests after key generation.
disable	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
tos	Value of the ToS byte in the IP datagram header .	integer	Minimum value: 0 Maximum value: 15
priority	ToS based priority level to low, medium or high .	option	-

Option	Description
low	Low priority.
medium	Medium priority.
high	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
ds	DSCP.	integer	Minimum value: 0 Maximum value: 63
priority	DSCP based priority level.	option	-

Option	Description
low	Low priority.
medium	Medium priority.
high	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
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024
ttl-mode	Mode for TWAMP packet TTL modification.	option	-

Option	Description
reinit	Reinitialize TTL.
decrease	Decrease TTL.
retain	Retain TTL.

mode	SLA response mode.	option	-

Option	Description
none	Disable probe.
http-probe	HTTP probe.
twamp	Two way active measurement protocol.

security-mode	Twamp respondor security mode.	option	-

Option	Description
none	Unauthenticated mode.
authentication	Authenticated mode.

Parameter	Description	Type	Size
password	Twamp respondor password in authentication mode	password	Not Specified
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600

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 <address1>, <address2>, ...
      set protocol {option1}, {option2}, ...
      set port {integer}
      set gateway-ip {ipv4-address-any}
      set gateway-ip6 {ipv6-address}
      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 security-mode [none|authentication]
      set password {password}
      set packet-size {integer}
      set ha-priority {integer}
      set update-cascade-interface [enable|disable]
      set update-static-route [enable|disable]
      set status [enable|disable]
   next
end
```

config system link-monitor

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

Option	Description
ipv4	IPv4 mode.
ipv6	IPv6 mode.

Parameter	Description	Type	Size
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15
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	-

Option	Description
ping	PING link monitor.
tcp-echo	TCP echo link monitor.
udp-echo	UDP echo link monitor.
http	HTTP-GET link monitor.
twamp	TWAMP link monitor.
ping6	PING6 link monitor.

port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535
gateway-ip	Gateway IP address used to probe the server.	ipv4-address-any	Not Specified
gateway-ip6	Gateway IPv6 address used to probe the server.	ipv6-address	Not Specified
source-ip	Source IP address used in packet to the server.	ipv4-address-any	Not Specified
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
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

Parameter	Description	Type	Size
probe-timeout	Time to wait before a probe packet is considered lost .	integer	Minimum value: 500 Maximum value: 5000
failtime	Number of retry attempts before the server is considered down	integer	Minimum value: 1 Maximum value: 3600
recoverytime	Number of successful responses received before server is considered recovered .	integer	Minimum value: 1 Maximum value: 3600
security-mode	Twamp controller security mode.	option	-

Option	Description
none	Unauthenticated mode.
authentication	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
ha-priority	HA election priority .	integer	Minimum value: 1 Maximum value: 50
update-cascade-interface	Enable/disable update cascade interface.	option	-

Option	Description
enable	Enable update cascade interface.
disable	Disable update cascade interface.

update-static-route	Enable/disable updating the static route.	option	-

Option	Description
enable	Enable updating the static route.
disable	Disable updating the static route.

Parameter	Description	Type	Size
status	Enable/disable this link monitor.	option	-

Option	Description
enable	Enable this link monitor.
disable	Disable this link monitor.

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
auto-install-config	Enable/disable auto install the config in USB disk.	option	-

Option	Description
enable	Enable config.
disable	Disable config.

Parameter	Description	Type	Size
auto-install-image	Enable/disable auto install the image in USB disk.	option	-

Option	Description
enable	Enable config.
disable	Disable config.

Parameter	Description	Type	Size
default-config-file	Default config file name in USB disk.	string	Maximum length: 127
default-image-file	Default image file name in USB disk.	string	Maximum length: 127

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
mode	Console mode.	option	-

Option	Description
batch	Batch mode.
line	Line mode.

baudrate	Console baud rate.	option	-

Option	Description
9600	9600
19200	19200
38400	38400
57600	57600
115200	115200

output	Console output mode.	option	-

Option	Description
standard	Standard output.
more	More page output.

login	Enable/disable serial console and FortiExplorer.	option	-

Option	Description
enable	Console login enable.
disable	Console login disable.

Parameter	Description	Type	Size
fortiexplorer *	Enable/disable access for FortiExplorer.	option	-

Option	Description
enable	Enable FortiExplorer access.
disable	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
ntpsync	Enable/disable setting the FortiGate system time by synchronizing with an NTP Server.	option	-

Parameter	Description	Type	Size
	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	-
	Option / **Description** *fortiguard* / Use the FortiGuard NTP server. *custom* / Use any other available NTP server.		
syncinterval	NTP synchronization interval .	integer	Minimum value: 1 Maximum value: 1440
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified
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	-
	Option / **Description** *enable* / Enable FortiGate NTP Server Mode. *disable* / Disable FortiGate NTP Server Mode.		
authentication	Enable/disable authentication.	option	-
	Option / **Description** *enable* / Enable authentication. *disable* / Disable authentication.		
key-type	Key type for authentication (MD5, SHA1).	option	-
	Option / **Description** *MD5* / Use MD5 to authenticate the message. *SHA1* / Use SHA1 to authenticate the message.		

Parameter	Description	Type	Size
key	Key for authentication.	password	Not Specified
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295
interface <interface-name>	FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79

config ntpserver

Parameter	Description	Type	Size
server	IP address or hostname of the NTP Server.	string	Maximum length: 63
ntpv3	Enable to use NTPv3 instead of NTPv4.	option	-

Option	Description
enable	Enable NTPv3.
disable	Disable NTPv3 (use NTPv4).

authentication	Enable/disable MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-

Option	Description
enable	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.
disable	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
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Option	Description
auto	Set outgoing interface automatically.

Parameter	Description	Type	Size
	Option / **Description** *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 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}
end
```

config system ptp

Parameter	Description	Type	Size
status	Enable/disable setting the FortiGate system time by synchronizing with an PTP Server.	option	-
	Option / **Description** *enable* — Enable synchronization with PTP Server. *disable* — Disable synchronization with PTP Server.		
mode	Multicast transmission or hybrid transmission.	option	-
	Option / **Description** *multicast* — Send PTP packets with multicast. *hybrid* — Send PTP packets with unicast and multicast.		
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-
	Option / **Description** *E2E* — End to end delay detection. *P2P* — Peer to peer delay detection.		

Parameter	Description	Type	Size
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
interface	PTP slave will reply through this interface.	string	Maximum length: 15

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
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
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

Parameter	Description	Type	Size
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
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	-

Option	Description
source	Source port match.
destination	Destination port match.

Parameter	Description	Type	Size
server-type	Cache server type.	option	-

Option	Description
forward	Forward server.
proxy	Proxy server.

Parameter	Description	Type	Size
ports	Service ports.	user	Not Specified
authentication	Enable/disable MD5 authentication.	option	-

Option	Description
enable	Enable MD5 authentication.
disable	Disable MD5 authentication.

Parameter	Description	Type	Size
password	Password for MD5 authentication.	password	Not Specified
forward-method	Method used to forward traffic to the cache servers.	option	-

Option	Description
GRE	GRE encapsulation.
L2	L2 rewrite.
any	GRE or L2.

Parameter	Description	Type	Size
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-

Parameter	Description	Type	Size
	Option / **Description** *GRE* / GRE encapsulation. *L2* / L2 rewrite.		
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-
	Option / **Description** *auto* / auto *standard* / Standard service. *dynamic* / Dynamic service.		
primary-hash	Hash method.	option	-
	Option / **Description** *src-ip* / Source IP hash. *dst-ip* / Destination IP hash. *src-port* / Source port hash. *dst-port* / Destination port hash.		
priority	Service priority.	integer	Minimum value: 0 Maximum value: 255
protocol	Service protocol.	integer	Minimum value: 0 Maximum value: 255
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-
	Option / **Description** *wccp-v2* / WCCP-v2 bucket format. *cisco-implementation* / Cisco bucket format.		

Parameter	Description	Type	Size
return-method	Method used to decline a redirected packet and return it to the FortiGate.	option	-

Option	Description
GRE	GRE encapsulation.
L2	L2 rewrite.
any	GRE or L2.

Parameter	Description	Type	Size
assignment-method	Hash key assignment preference.	option	-

Option	Description
HASH	HASH assignment method.
MASK	MASK assignment method.
any	HASH or MASK.

Parameter	Description	Type	Size
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified

config system nat64

Configure NAT64.

```
config system nat64
   Description: Configure NAT64.
   set status [enable|disable]
   set nat64-prefix {ipv6-prefix}
   set secondary-prefix-status [enable|disable]
   config secondary-prefix
      Description: Secondary NAT64 prefix.
      edit <name>
         set nat64-prefix {ipv6-prefix}
      next
   end
   set always-synthesize-aaaa-record [enable|disable]
   set generate-ipv6-fragment-header [enable|disable]
   set nat46-force-ipv4-packet-forwarding [enable|disable]
end
```

config system nat64

Parameter	Description	Type	Size
status	Enable/disable NAT64 .	option	-

Option	Description
enable	Enable NAT64.
disable	Disable NAT64.

Parameter	Description	Type	Size
nat64-prefix	NAT64 prefix must be ::/96 .	ipv6-prefix	Not Specified
secondary-prefix-status	Enable/disable secondary NAT64 prefix.	option	-

Option	Description
enable	Enable secondary NAT64.
disable	Disable secondary NAT64.

Parameter	Description	Type	Size
always-synthesize-aaaa-record	Enable/disable AAAA record synthesis .	option	-

Option	Description
enable	Enable AAAA record synthesis.
disable	Disable AAAA record synthesis.

Parameter	Description	Type	Size
generate-ipv6-fragment-header	Enable/disable IPv6 fragment header generation.	option	-

Option	Description
enable	Enable IPv6 fragment header generation.
disable	Disable IPv6 fragment header generation.

Parameter	Description	Type	Size
nat46-force-ipv4-packet-forwarding	Enable/disable mandatory IPv4 packet forwarding in nat46.	option	-

Option	Description
enable	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.
disable	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.

config secondary-prefix

Parameter	Description	Type	Size
nat64-prefix	NAT64 prefix.	ipv6-prefix	Not Specified

config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
   Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for
        this VDOM.
   edit <name>
      set status [enable|disable]
      set radius-server-vdom {string}
   next
end
```

config system vdom-radius-server

Parameter	Description	Type	Size
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-

Option	Description
enable	Enable the RSSO RADIUS server for this VDOM.
disable	Disable the RSSO RADIUS server for this VDOM.

radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31

config system 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-ip {ipv4-address}
   set status [enable|disable]
end
```

config system ftm-push

Parameter	Description	Type	Size
server-port	Port to communicate with FortiToken Mobile push services server .	integer	Minimum value: 1 Maximum value: 65535
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
status	Enable/disable the use of FortiToken Mobile push services.	option	-

Parameter	Description	Type	Size

Option	Description
enable	Enable FortiToken Mobile push services.
disable	Disable FortiToken Mobile push services.

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
   next
end
```

config system geoip-override

Parameter	Description	Type	Size
description	Description.	string	Maximum length: 127
country-id	Two character Country ID code.	string	Maximum length: 2

config ip-range

Parameter	Description	Type	Size
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
end-ip	Final IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified

config system fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
   Description: Configure FortiSandbox.
   set status [enable|disable]
   set server {string}
   set source-ip {string}
   set enc-algorithm [default|high|...]
   set ssl-min-proto-version [default|SSLv3|...]
   set email {string}
end
```

config system fortisandbox

Parameter	Description	Type	Size
status	Enable/disable FortiSandbox.	option	-

Option	Description
enable	Enable FortiSandbox.
disable	Disable FortiSandbox.

Parameter	Description	Type	Size
server	Server address of the remote FortiSandbox.	string	Maximum length: 63
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-

Option	Description
default	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.

Parameter	Description	Type	Size
	Option / **Description** *TLSv1-1* / TLSv1.1. *TLSv1-2* / TLSv1.2.		
email	Notifier email address.	string	Maximum length: 63

config system vdom-exception

Global configuration objects that can be configured independently for all VDOMs or for the defined VDOM scope.

```
config system vdom-exception
   Description: Global configuration objects that can be configured independently 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
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-

Option	Description
log.fortianalyzer.setting	log.fortianalyzer.setting
log.fortianalyzer.override-setting	log.fortianalyzer.override-setting
log.fortianalyzer2.setting	log.fortianalyzer2.setting
log.fortianalyzer2.override-setting	log.fortianalyzer2.override-setting
log.fortianalyzer3.setting	log.fortianalyzer3.setting
log.fortianalyzer3.override-setting	log.fortianalyzer3.override-setting
log.fortianalyzer-cloud.setting	log.fortianalyzer-cloud.setting

Parameter	Description	Type	Size
	Option / **Description** *log.fortianalyzer-cloud.override-setting* — log.fortianalyzer-cloud.override-setting *system.central-management* — system.central-management *system.csf* — system.csf *user.radius* — user.radius		
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-
	Option / **Description** *all* — Object configuration independent for all VDOMs. *inclusive* — Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration. *exclusive* — 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 configuration-sync [default|local]
   set management-ip {string}
   set management-port {integer}
   config trusted-list
      Description: Pre-authorized and blocked security fabric nodes.
      edit <serial>
         set action [accept|deny]
         set ha-members {string}
         set downstream-authorization [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
status	Enable/disable Security Fabric.	option	-

Option	Description
enable	Enable Security Fabric.
disable	Disable Security Fabric.

Parameter	Description	Type	Size
upstream-ip	IP address of the FortiGate upstream from this FortiGate in the Security Fabric.	ipv4-address	Not Specified
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
group-name	Security Fabric group name. All FortiGates in a Security Fabric must have the same group name.	string	Maximum length: 35
group-password	Security Fabric group password. All FortiGates in a Security Fabric must have the same group password.	password	Not Specified
configuration-sync	Configuration sync mode.	option	-

Option	Description
default	Synchronize configuration for FortiAnalyzer, FortiSandbox and Central Management to root node.
local	Do not synchronize configuration with root node.

Parameter	Description	Type	Size
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: 0 Maximum value: 65535

config trusted-list

Parameter	Description	Type	Size
action	Security fabric authorization action.	option	-

Option	Description
accept	Accept authorization request.
deny	Deny authorization request.

Parameter	Description	Type	Size
ha-members	HA members.	string	Maximum length: 19
downstream-authorization	Trust authorizations by this node's administrator.	option	-

Option	Description
enable	Enable downstream authorization.
disable	Disable downstream authorization.

config fabric-device

Parameter	Description	Type	Size
device-ip	Device IP.	ipv4-address	Not Specified
https-port	HTTPS port for fabric device.	integer	Minimum value: 1 Maximum value: 65535
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 trigger-type [event-based|scheduled]
      set event-type [ioc|event-log|...]
      set license-type [forticare-support|fortiguard-webfilter|...]
      set ioc-level [medium|high]
      set logid {integer}
      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}
   next
end
```

config system automation-trigger

Parameter	Description	Type	Size
trigger-type	Trigger type.	option	-

Option	Description
event-based	Event based trigger.
scheduled	Scheduled trigger.

Parameter	Description	Type	Size
event-type	Event type.	option	-

Option	Description
ioc	Indicator of compromise detected.
event-log	Use log ID as trigger.
reboot	Device reboot.
low-memory	Conserve mode due to low memory.
high-cpu	High CPU usage.
license-near-expiry	License near expiration date.
ha-failover	HA failover.
config-change	Configuration change.
security-rating-summary	Security rating summary.
virus-ips-db-updated	Virus and IPS database updated.
faz-event	FortiAnalyzer event.

Parameter	Description	Type	Size
license-type	License type.	option	-

Parameter	Description	Type	Size
	Option / **Description** *forticare-support* — FortiCare support license. *fortiguard-webfilter* — FortiGuard web filter license. *fortiguard-antispam* — FortiGuard antispam license. *fortiguard-antivirus* — FortiGuard AntiVirus license. *fortiguard-ips* — FortiGuard IPS license. *fortiguard-management* — FortiGuard management service license. *forticloud* — FortiCloud license.		
ioc-level	IOC threat level.	option	-
	Option / **Description** *medium* — IOC level medium and high. *high* — IOC level high only.		
logid	Log ID to trigger event.	integer	Minimum value: 1 Maximum value: 65535
trigger-frequency	Scheduled trigger frequency .	option	-
	Option / **Description** *hourly* — Run hourly. *daily* — Run daily. *weekly* — Run weekly. *monthly* — Run monthly.		
trigger-weekday	Day of week for trigger.	option	-
	Option / **Description** *sunday* — Sunday.		

Parameter	Description	Type	Size
	Option / **Description** *monday* / Monday. *tuesday* / Tuesday. *wednesday* / Wednesday. *thursday* / Thursday. *friday* / Friday. *saturday* / Saturday.		
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31
trigger-hour	Hour of the day on which to trigger .	integer	Minimum value: 0 Maximum value: 23
trigger-minute	Minute of the hour on which to trigger .	integer	Minimum value: 0 Maximum value: 59
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

config fields

Parameter	Description	Type	Size
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 action-type [email|ios-notification|...]
       set tls-certificate {string}
       set email-to <name1>, <name2>, ...
       set email-from {var-string}
       set email-subject {var-string}
       set email-body {string}
       set minimum-interval {integer}
       set delay {integer}
       set required [enable|disable]
       set aws-api-id {string}
       set aws-region {string}
       set aws-domain {string}
       set aws-api-stage {string}
       set aws-api-path {string}
       set aws-api-key {password}
       set azure-app {string}
       set azure-function {string}
       set azure-domain {string}
       set azure-function-authorization [anonymous|function|...]
       set azure-api-key {password}
       set gcp-function-region {string}
       set gcp-project {string}
       set gcp-function-domain {string}
       set gcp-function {string}
       set alicloud-account-id {string}
       set alicloud-region {string}
       set alicloud-function-domain {string}
       set alicloud-version {string}
       set alicloud-service {string}
       set alicloud-function {string}
       set alicloud-function-authorization [anonymous|function]
       set alicloud-access-key-id {string}
       set alicloud-access-key-secret {password}
       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 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
action-type	Action type.	option	-

Parameter	Description	Type	Size
	Option — **Description** *email* — Send notification email. *ios-notification* — Send push notification to FortiExplorer iOS. *alert* — Generate FortiOS dashboard alert. *disable-ssid* — Disable interface. *quarantine* — Quarantine host. *quarantine-forticlient* — Quarantine FortiClient by EMS. *quarantine-nsx* — Quarantine NSX instance. *ban-ip* — Ban IP address. *aws-lambda* — Send log data to integrated AWS service. *azure-function* — Send log data to an Azure function. *google-cloud-function* — Send log data to a Google Cloud function. *alicloud-function* — Send log data to an AliCloud function. *webhook* — Send an HTTP request. *cli-script* — Run CLI script.		
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35
email-to <name>	Email addresses. Email address.	string	Maximum length: 255
email-from	Email sender name.	var-string	Maximum length: 127
email-subject	Email subject.	var-string	Maximum length: 511
email-body	Email body.	string	Maximum length: 1023
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000

Parameter	Description	Type	Size
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600
required	Required in action chain.	option	-

Option	Description
enable	Required in action chain.
disable	Not required in action chain.

aws-api-id	AWS API Gateway ID.	string	Maximum length: 35
aws-region	AWS region.	string	Maximum length: 35
aws-domain	AWS domain.	string	Maximum length: 63
aws-api-stage	AWS API Gateway deployment stage name.	string	Maximum length: 63
aws-api-path	AWS API Gateway path.	string	Maximum length: 63
aws-api-key	AWS API Gateway API key.	password	Not Specified
azure-app	Azure function application name.	string	Maximum length: 63
azure-function	Azure function name.	string	Maximum length: 63
azure-domain	Azure function domain.	string	Maximum length: 63
azure-function-authorization	Azure function authorization level.	option	-

Option	Description
anonymous	Anonymous authorization level (No authorization required).
function	Function authorization level (Function or Host Key required).
admin	Admin authorization level (Master Host Key required).

azure-api-key	Azure function API key.	password	Not Specified
gcp-function-region	Google Cloud function region.	string	Maximum length: 63

Parameter	Description	Type	Size
gcp-project	Google Cloud Platform project name.	string	Maximum length: 63
gcp-function-domain	Google Cloud function domain.	string	Maximum length: 63
gcp-function	Google Cloud function name.	string	Maximum length: 63
alicloud-account-id	AliCloud account ID.	string	Maximum length: 63
alicloud-region	AliCloud region.	string	Maximum length: 63
alicloud-function-domain	AliCloud function domain.	string	Maximum length: 63
alicloud-version	AliCloud version.	string	Maximum length: 63
alicloud-service	AliCloud service name.	string	Maximum length: 128
alicloud-function	AliCloud function name.	string	Maximum length: 128
alicloud-function-authorization	AliCloud function authorization type.	option	-

Option	Description
anonymous	Anonymous authorization (No authorization required).
function	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
protocol	Request protocol.	option	-

Option	Description
http	HTTP.
https	HTTPS.

Parameter	Description	Type	Size
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-

Option	Description
post	POST.
put	PUT.
get	GET.
patch	PATCH.
delete	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: 1023
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535
headers <header>	Request headers. Request header.	string	Maximum length: 255
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
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
type	Destination type.	option	-

Option	Description
fortigate	FortiGate set as destination.
ha-cluster	HA cluster set as destination.

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

config system automation-stitch

Automation stitches.

```
config system automation-stitch
   Description: Automation stitches.
   edit <name>
      set status [enable|disable]
      set trigger {string}
      set action <name1>, <name2>, ...
      set destination <name1>, <name2>, ...
   next
end
```

config system automation-stitch

Parameter	Description	Type	Size
status	Enable/disable this stitch.	option	-

Option	Description
enable	Enable stitch.
disable	Disable stitch.

trigger	Trigger name.	string	Maximum length: 35
action <name>	Action names. Action name.	string	Maximum length: 79

Parameter	Description	Type	Size
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79

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
status	Enable/disable neighbor discovery proxy.	option	-

Option	Description
enable	Enable neighbor discovery proxy.
disable	Disable neighbor discovery proxy.

Parameter	Description	Type	Size
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 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-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
status	Enable/disable SAML authentication .	option	-
	Option / **Description** *enable* — Enable SAML authentication. *disable* — Disable SAML authentication.		
role	SAML role.	option	-
	Option / **Description** *identity-provider* — Identity Provider. *service-provider* — Service Provider.		
default-login-page	Choose default login page.	option	-
	Option / **Description** *normal* — Use local login page as default. *sso* — Use IdP's Single Sign-On page as default.		
default-profile	Default profile for new SSO admin.	string	Maximum length: 35

Parameter	Description	Type	Size
cert	Certificate to sign SAML messages.	string	Maximum length: 35
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
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295

config service-providers

Parameter	Description	Type	Size
prefix	Prefix.	string	Maximum length: 35
sp-cert	SP certificate name.	string	Maximum length: 35

Parameter	Description	Type	Size
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
type	Type.	option	-

Option	Description
username	User Name.
email	Email address.

test

This section includes syntax for the following commands:

- config test lnkmtd on page 1087
- config test pptpcd on page 1082
- config test fsd on page 1084
- config test sflowd on page 1081
- config test ddnscd on page 1080
- config test ipmc_sensord on page 1087
- config test bfd on page 1093
- config test ipsengine on page 1079
- config test wad on page 1083
- config test autod on page 1093
- config test snmpd on page 1080
- config test fas on page 1094
- config test radiusd on page 1083
- config test info-sslvpnd on page 1086
- config test imap on page 1075
- config test sdncd on page 1091
- config test harelay on page 1076
- config test ipldbd on page 1079
- config test wccpd on page 1083
- config test dhcp6r on page 1088
- config test ipsufd on page 1084
- config test fnbamd on page 1089
- config test dhcprelay on page 1082
- config test radvd on page 1091
- config test l2tpcd on page 1082
- config test ocid on page 1092
- config test urlfilter on page 1078
- config test ipsmonitor on page 1079
- config test quarantined on page 1086
- config test miglogd on page 1077
- config test netxd on page 1088
- config test fcnacd on page 1091
- config test smtp on page 1074
- config test lted on page 1084
- config test acd on page 1080
- config test sessionsync on page 1077
- config test dsd on page 1087
- config test fsvrd on page 1090
- config test init on page 1081

- config test sepmd on page 1095
- config test hasync on page 1076
- config test pop3 on page 1075
- config test dhcp6c on page 1086
- config test zebos_launcher on page 1089
- config test nntp on page 1075
- config test forticron on page 1085
- config test csfd on page 1090
- config test kubed on page 1093
- config test awsd on page 1088
- config test gcpd on page 1092
- config test ftpd on page 1074
- config test dnsproxy on page 1081
- config test mrd on page 1089
- config test wf_monitor on page 1078
- config test forticldd on page 1077
- config test uploadd on page 1085
- config test vmwd on page 1094
- config test ovrd on page 1078
- config test azd on page 1092
- config test openstackd on page 1094
- config test hatalk on page 1076
- config test radius-das on page 1090

config test smtp

SMTP proxy.

```
config test smtp
   Description: SMTP proxy.
   set <Integer> {string}
end
```

config test smtp

Parameter	Description	Type	Size
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<Integer>	Test level.	string	Maximum length: -1

config test lted

This command is available for reference model(s) FortiGate 80E-POE, FortiGate 501E, FortiGate 3000D, FortiWiFi 61E. 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
<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
<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
<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
<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
<Integer>	Test level.	string	Maximum length: -1

config test info-sslvpnd

SSL-VPN info daemon.

```
config test info-sslvpnd
   Description: SSL-VPN info daemon.
   set <Integer> {string}
end
```

config test info-sslvpnd

Parameter	Description	Type	Size
<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
<Integer>	Test level.	string	Maximum length: -1

config test ipmc_sensord

This command is available for reference model(s) FortiGate 80E-POE, FortiGate 501E, FortiGate 3000D. It is not available for FortiGate VM64, FortiWiFi 61E.

Ipmc sensor daemon.

```
config test ipmc_sensord
   Description: Ipmc sensor daemon.
   set <Integer> {string}
end
```

config test ipmc_sensord

Parameter	Description	Type	Size
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<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
<Integer>	Test level.	string	Maximum length: -1

config test sdncd

SDN Connector daemon.

```
config test sdncd
   Description: SDN Connector daemon.
   set <Integer> {string}
end
```

config test sdncd

Parameter	Description	Type	Size
<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
<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
<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
<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
<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
<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
<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
<Integer>	Test level.	string	Maximum length: -1

config test vmwd

VMware vSphere daemon.

```
config test vmwd
   Description: VMware vSphere daemon.
   set <Integer> {string}
end
```

config test vmwd

Parameter	Description	Type	Size
<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
<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
<Integer>	Test level.	string	Maximum length: -1

user

This section includes syntax for the following commands:

- config user fortitoken on page 1123
- config user group on page 1135
- config user security-exempt-list on page 1140
- config user adgrp on page 1121
- config user exchange on page 1108
- config user fsso-polling on page 1122
- config user domain-controller on page 1115
- config user saml on page 1117
- config user pop3 on page 1116
- config user krb-keytab on page 1114
- config user peergrp on page 1134
- config user quarantine on page 1134
- config user local on page 1125
- config user tacacs+ on page 1106
- config user fsso on page 1118
- config user setting on page 1128
- config user password-policy on page 1124
- config user peer on page 1132
- config user ldap on page 1110
- config user radius on page 1096

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 class <name1>, <name2>, ...
      set password-renewal [enable|disable]
      set password-encoding [auto|ISO-8859-1]
      set acct-all-servers [enable|disable]
      set interface-select-method [auto|sdwan|...]
      set interface {string}
      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
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
secondary-secret	Secret key to access the secondary server.	password	Not Specified

Parameter	Description	Type	Size
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
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-

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	-

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
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 600 Maximum value: 86400
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-

Option	Description
enable	Enable RADIUS CoA.
disable	Disable RADIUS CoA.

radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-

Option	Description
enable	Enable H3C compatibility.
disable	Disable H3C compatibility.

Parameter	Description	Type	Size
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-

Option	Description
auto	Use PAP, MSCHAP_v2, and CHAP (in that order).
ms_chap_v2	Microsoft Challenge Handshake Authentication Protocol version 2.
ms_chap	Microsoft Challenge Handshake Authentication Protocol.
chap	Challenge Handshake Authentication Protocol.
pap	Password Authentication Protocol.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable username case-sensitive.
disable	Disable username case-sensitive.

Parameter	Description	Type	Size
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79
password-renewal	Enable/disable password renewal.	option	-

Option	Description
enable	Enable password renewal.
disable	Disable password renewal.

Parameter	Description	Type	Size
password-encoding	Password encoding.	option	-

Parameter	Description	Type	Size
	Option / **Description** *auto* — Use original password encoding. *ISO-8859-1* — Use ISO-8859-1 password encoding.		
acct-all-servers	Enable/disable sending of accounting messages to all configured servers .	option	-
	Option / **Description** *enable* — Send accounting messages to all configured servers. *disable* — Send accounting message only to servers that are confirmed to be reachable.		
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	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
rsso	Enable/disable RADIUS based single sign on feature.	option	-
	Option / **Description** *enable* — Enable RADIUS based single sign on feature. *disable* — 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
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-
	Option / **Description** *enable* — Enable sending RADIUS response packets. *disable* — Disable sending RADIUS response packets.		

Parameter	Description	Type	Size
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-

Option	Description
enable	Enable validating RADIUS request shared secret.
disable	Disable validating RADIUS request shared secret.

rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified
rsso-endpoint-attribute	RADIUS attributes used to extract the user end point identifer from the RADIUS Start record.	option	-

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
Class	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.

Parameter	Description	Type	Size
	Option / **Description** *Login-LAT-Service* / Use this attribute. *Login-LAT-Node* / Use this attribute. *Login-LAT-Group* / Use this attribute. *Framed-AppleTalk-Zone* / Use this attribute. *Acct-Session-Id* / Use this attribute. *Acct-Multi-Session-Id* / Use this attribute.		
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-
	Option / **Description** *User-Name* / Use this attribute. *NAS-IP-Address* / Use this attribute. *Framed-IP-Address* / Use this attribute. *Framed-IP-Netmask* / Use this attribute. *Filter-Id* / Use this attribute. *Login-IP-Host* / Use this attribute. *Reply-Message* / Use this attribute. *Callback-Number* / Use this attribute. *Callback-Id* / Use this attribute. *Framed-Route* / Use this attribute. *Framed-IPX-Network* / Use this attribute. *Class* / Use this attribute. *Called-Station-Id* / Use this attribute.		

Parameter	Description	Type	Size

Option	Description
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Session-Id	Use this attribute.
Acct-Multi-Session-Id	Use this attribute.

sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.

Parameter	Description	Type	Size
	Option / **Description** *Framed-IPX-Network* — Use this attribute. *Class* — Use this attribute. *Called-Station-Id* — Use this attribute. *Calling-Station-Id* — Use this attribute. *NAS-Identifier* — Use this attribute. *Proxy-State* — Use this attribute. *Login-LAT-Service* — Use this attribute. *Login-LAT-Node* — Use this attribute. *Login-LAT-Group* — Use this attribute. *Framed-AppleTalk-Zone* — Use this attribute. *Acct-Session-Id* — Use this attribute. *Acct-Multi-Session-Id* — Use this attribute.		
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	-
	Option / **Description** *enable* — Enable override old attribute value with new value for the same endpoint. *disable* — Disable override old attribute value with new value for the same endpoint.		
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

Parameter	Description	Type	Size
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
rsso-log-flags	Events to log.	option	-

Option	Description
protocol-error	Enable this log type.
profile-missing	Enable this log type.
accounting-stop-missed	Enable this log type.
accounting-event	Enable this log type.
endpoint-block	Enable this log type.
radiusd-other	Enable this log type.
none	Disable all logging.

Parameter	Description	Type	Size
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-

Option	Description
enable	Enable flush user IP sessions on RADIUS accounting stop.
disable	Disable flush user IP sessions on RADIUS accounting stop.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.
disable	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.

config accounting-server

Parameter	Description	Type	Size
status	Status.	option	-

Parameter	Description	Type	Size
	Option: *enable* — Log to remote syslog server. Option: *disable* — 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
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	-
	Option: *auto* — Set outgoing interface automatically. Option: *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. Option: *specify* — 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
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
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	-

Option	Description
mschap	MSCHAP.
chap	CHAP.
pap	PAP.
ascii	ASCII.
auto	Use PAP, MSCHAP, and CHAP (in that order).

authorization	Enable/disable TACACS+ authorization.	option	-

Option	Description
enable	Enable TACACS+ authorization.
disable	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	-

Option	Description
auto	Set outgoing interface automatically.

Parameter	Description	Type	Size
	Option / **Description** *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 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 kdc-ip <ipv41>, <ipv42>, ...
   next
end
```

config user exchange

Parameter	Description	Type	Size
server-name	MS Exchange server hostname.	string	Maximum length: 63
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64
password	Password for the specified username.	password	Not Specified
ip	Server IPv4 address.	ipv4-address-any	Not Specified
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-

Parameter	Description	Type	Size
	Option / **Description** *rpc-over-tcp* — Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013. *rpc-over-http* — Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013. *rpc-over-https* — 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	-
	Option / **Description** *spnego* — Negotiate authentication. *ntlm* — NTLM authentication. *kerberos* — Kerberos authentication.		
auth-level	Authentication security level used for the RPC protocol layer.	option	-
	Option / **Description** *connect* — RPC authentication level 'connect'. *call* — RPC authentication level 'call'. *packet* — RPC authentication level 'packet'. *integrity* — RPC authentication level 'integrity'. *privacy* — RPC authentication level 'privacy'.		
http-auth-type	Authentication security type used for the HTTP transport.	option	-
	Option / **Description** *basic* — Basic HTTP authentication. *ntlm* — NTLM HTTP authentication.		
ssl-min-proto-version	Minimum SSL/TLS protocol version for HTTPS transport .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3.		

Parameter	Description	Type	Size
	Option — **Description** *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.		
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 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}
   next
end
```

config user ldap

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable server identity check.
disable	Disable server identity check.

source-ip	Source IP for communications to LDAP server.	ipv4-address	Not Specified
cnid	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is "cn".	string	Maximum length: 20
dn	Distinguished name used to look up entries on the LDAP server.	string	Maximum length: 511
type	Authentication type for LDAP searches.	option	-

Option	Description
simple	Simple password authentication without search.
anonymous	Bind using anonymous user search.
regular	Bind using username/password and then search.

two-factor	Enable/disable two-factor authentication.	option	-

Option	Description
disable	disable two-factor authentication.
fortitoken-cloud	FortiToken Cloud Service.

two-factor-authentication	Authentication method by FortiToken Cloud.	option	-

Parameter	Description	Type	Size
	Option / **Description** *fortitoken* / FortiToken authentication. *email* / Email one time password. *sms* / SMS one time password.		
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-
	Option / **Description** *email* / Email notification for activation code. *sms* / 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	-
	Option / **Description** *user-attr* / User attribute checking. *group-object* / Group object checking. *posix-group-object* / POSIX group object checking.		
group-search-base	Search base used for group searching.	string	Maximum length: 511
group-object-filter	Filter used for group searching.	string	Maximum length: 2047
group-filter	Filter used for group matching.	string	Maximum length: 2047
secure	Port to be used for authentication.	option	-
	Option / **Description** *disable* / No SSL. *starttls* / Use StartTLS. *ldaps* / Use LDAPS.		

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
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
password-expiry-warning	Enable/disable password expiry warnings.	option	-

Option	Description
enable	Enable password expiry warnings.
disable	Disable password expiry warnings.

Parameter	Description	Type	Size
password-renewal	Enable/disable online password renewal.	option	-

Option	Description
enable	Enable online password renewal.
disable	Disable online password renewal.

Parameter	Description	Type	Size
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-

Option	Description
same	Same as UPN.
strip	Strip domain string from UPN.

Parameter	Description	Type	Size
account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047
search-type	Search type.	option	-

Option	Description
recursive	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	-

Option	Description
enable	Enable obtaining of user information.
disable	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	-

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 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 {string}
      set keytab {string}
   next
end
```

config user krb-keytab

Parameter	Description	Type	Size
pac-data	Enable/disable parsing PAC data in the ticket.	option	-

Option	Description
enable	Enable parsing PAC data in the ticket.
disable	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	LDAP server name.	string	Maximum length: 35
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 ip-address {ipv4-address}
      set port {integer}
      config extra-server
         Description: extra servers.
         edit <id>
            set ip-address {ipv4-address}
            set port {integer}
         next
      end
      set domain-name {string}
      set ldap-server {string}
   next
end
```

config user domain-controller

Parameter	Description	Type	Size
ip-address	Domain controller IP address.	ipv4-address	Not Specified
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
domain-name	Domain DNS name.	string	Maximum length: 255
ldap-server	LDAP server name.	string	Maximum length: 35

config extra-server

Parameter	Description	Type	Size
ip-address	Domain controller IP address.	ipv4-address	Not Specified
port	Port to be used for communication with the domain controller .	integer	Minimum value: 0 Maximum value: 65535

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
server	{<name_str|ip_str>} server domain name or IP.	string	Maximum length: 63
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535
secure	SSL connection.	option	-

Option	Description
none	None.

Parameter	Description	Type	Size
	Option / **Description** *starttls* — Use StartTLS. *pop3s* — Use POP3 over SSL.		
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — 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}
   next
end
```

config user saml

Parameter	Description	Type	Size
cert	Certificate to sign SAML messages.	string	Maximum length: 35
entity-id	SP entity ID.	string	Maximum length: 255

Parameter	Description	Type	Size
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: 35
group-name	Group name in assertion statement.	string	Maximum length: 35

config user fsso

Configure Fortinet Single Sign On (FSSO) agents.

```
config user fsso
   Description: Configure Fortinet Single Sign On (FSSO) agents.
   edit <name>
      set type [default|fortiems|...]
      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 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 fsso

Parameter	Description	Type	Size
type	Server type.	option	-

Option	Description
default	All other unspecified types of servers.
fortiems	FortiClient EMS server.
fortinac	FortiNAC server.
fortiems-cloud	FortiClient EMS Cloud 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
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
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

Parameter	Description	Type	Size
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535
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
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535
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. The collector agent can only accept passwords up to 15 characters in length.	integer	Minimum value: 1 Maximum value: 65535
password5	Password of the fifth FSSO collector agent.	password	Not Specified
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
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-

Option	Description
enable	Enable automatic fetching of groups from LDAP server.
disable	Disable automatic fetching of groups from LDAP server.

Parameter	Description	Type	Size
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047
user-info-server	LDAP server to get user information.	string	Maximum length: 35
ssl	Enable/disable use of SSL.	option	-

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
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	-

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 id {integer}
   next
end
```

config user adgrp

Parameter	Description	Type	Size
server-name	FSSO agent name.	string	Maximum length: 35
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295

config user fsso-polling

Configure FSSO active directory servers for polling mode.

```
config user fsso-polling
   Description: Configure FSSO active directory servers for polling mode.
   edit <id>
      set status [enable|disable]
      set server {string}
      set default-domain {string}
      set port {integer}
      set user {string}
      set password {password}
      set ldap-server {string}
      set logon-history {integer}
      set polling-frequency {integer}
      config adgrp
         Description: LDAP Group Info.
         edit <name>
         next
      end
      set smbv1 [enable|disable]
      set smb-ntlmv1-auth [enable|disable]
   next
end
```

config user fsso-polling

Parameter	Description	Type	Size
status	Enable/disable polling for the status of this Active Directory server.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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
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
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30
smbv1	Enable/disable support of SMBv1 for Samba.	option	-

Option	Description
enable	Enable support of SMBv1 for Samba.
disable	Disable support of SMBv1 for Samba.

smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-

Option	Description
enable	Enable support of NTLMv1 for Samba authentication.
disable	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
status	Status	option	-

Option	Description
active	Activate FortiToken.
lock	Lock FortiToken.

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
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
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999
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
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-

Option	Description
enable	Enable renewal of a password that already is expired.
disable	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-case-sensitivity [disable|enable]
  next
end
```

config user local

Parameter	Description	Type	Size
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295
status	Enable/disable allowing the local user to authenticate with the FortiGate unit.	option	-

Option	Description
enable	Enable user.
disable	Disable user.

type	Authentication method.	option	-

Option	Description
password	Password authentication.
radius	RADIUS server authentication.
tacacs+	TACACS+ server authentication.
ldap	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
two-factor	Enable/disable two-factor authentication.	option	-

Option	Description
disable	disable
fortitoken	FortiToken
fortitoken-cloud	FortiToken Cloud Service.

Parameter	Description	Type	Size
	Option / **Description** *email* — Email authentication code. *sms* — SMS authentication code.		
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-
	Option / **Description** *fortitoken* — FortiToken authentication. *email* — Email one time password. *sms* — SMS one time password.		
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-
	Option / **Description** *email* — Email notification for activation code. *sms* — 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	-
	Option / **Description** *fortiguard* — Send SMS by FortiGuard. *custom* — Send SMS by custom server.		
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35
passwd-time	Time of the last password update.	user	Not Specified

Parameter	Description	Type	Size
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440
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	-

Option	Description
enable	Enable auth-concurrent-override.
disable	Disable auth-concurrent-override.

Parameter	Description	Type	Size
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100
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-case-sensitivity	Enable/disable case sensitivity when performing username matching (uppercase and lowercase letters are treated either as distinct or equivalent).	option	-

Option	Description
disable	Ignore case. Username at prompt not required to match case.
enable	Do not ignore case. Username at prompt must match case.

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
auth-type	Supported firewall policy authentication protocols/methods.	option	-

Option	Description
http	Allow HTTP authentication.
https	Allow HTTPS authentication.
ftp	Allow FTP authentication.
telnet	Allow TELNET authentication.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-
	Option / **Description** *enable* / Allow SSL re-negotiation. *disable* / Forbid SSL re-negotiation.		
auth-src-mac	Enable/disable source MAC for user identity.	option	-
	Option / **Description** *enable* / Enable source MAC for user identity. *disable* / Disable source MAC for user identity.		
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-
	Option / **Description** *always* / Always trigger firewall authentication on demand. *implicitly* / 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
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	-
	Option / **Description** *idle-timeout* / Idle timeout. *hard-timeout* / Hard timeout. *new-session* / New session timeout.		
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate .	integer	Minimum value: 1 Maximum value: 30

Parameter	Description	Type	Size
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-

Option	Description
hard-timeout	Use session timeout from RADIUS as hard-timeout.
ignore-timeout	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
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-

Option	Description
enable	Enable per policy disclaimer.
disable	Disable per policy disclaimer.

auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections .	option	-

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

config auth-ports

Parameter	Description	Type	Size
type	Service type.	option	-

Option	Description
http	HTTP service.
https	HTTPS service.
ftp	FTP service.
telnet	TELNET service.

port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535

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
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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / 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	-
	Option / **Description** *string* / Normal string. *email* / Email address. *FQDN* / Fully Qualified Domain Name. *ipv4* / IPv4 address. *ipv6* / 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	-
	Option / **Description** *password* / Username/password. *principal-name* / 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	-
	Option / **Description** *enable* / Enable 2-factor authentication.		

Parameter	Description	Type	Size
	Option: *disable* — Description: 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
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}
   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 parent {string}
            next
         end
      next
   end
end
```

config user quarantine

Parameter	Description	Type	Size
quarantine	Enable/disable quarantine.	option	-

Option	Description
enable	Enable quarantine.
disable	Disable quarantine.

Parameter	Description	Type	Size
traffic-policy	Traffic policy for quarantined MACs.	string	Maximum length: 63

config targets

Parameter	Description	Type	Size
description	Description for the quarantine entry.	string	Maximum length: 63

config macs

Parameter	Description	Type	Size
description	Description for the quarantine MAC.	string	Maximum length: 63
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
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-

Option	Description
firewall	Firewall.
fsso-service	Fortinet Single Sign-On Service.
rsso	RADIUS based Single Sign-On Service.
guest	Guest.

Parameter	Description	Type	Size
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
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-

Option	Description
enable	Enable auth-concurrent-override.
disable	Disable auth-concurrent-override.

auth-concurrent-value	Maximum number of concurrent authenticated connections per user .	integer	Minimum value: 0 Maximum value: 100
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511
member <name>	Names of users, peers, LDAP severs, or RADIUS servers to add to the user group. Group member name.	string	Maximum length: 511
user-id	Guest user ID type.	option	-

Option	Description
email	Email address.
auto-generate	Automatically generate.
specify	Specify.

password	Guest user password type.	option	-

Option	Description
auto-generate	Automatically generate.
specify	Specify.
disable	Disable.

user-name	Enable/disable the guest user name entry.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Enable setting. *enable* — Disable setting.		
sponsor	Set the action for the sponsor guest user field.	option	-
	Option / **Description** *optional* — Optional. *mandatory* — Mandatory. *disabled* — Disabled.		
company	Set the action for the company guest user field.	option	-
	Option / **Description** *optional* — Optional. *mandatory* — Mandatory. *disabled* — Disabled.		
email	Enable/disable the guest user email address field.	option	-
	Option / **Description** *disable* — Enable setting. *enable* — Disable setting.		
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-
	Option / **Description** *disable* — Enable setting. *enable* — Disable setting.		
sms-server	Send SMS through FortiGuard or other external server.	option	-
	Option / **Description** *fortiguard* — Send SMS by FortiGuard. *custom* — Send SMS by custom server.		
sms-custom-server	SMS server.	string	Maximum length: 35

Parameter	Description	Type	Size
expire-type	Determine when the expiration countdown begins.	option	-

Option	Description
immediately	Immediately.
first-successful-login	First successful login.

Parameter	Description	Type	Size
expire	Time in seconds before guest user accounts expire.	integer	Minimum value: 1 Maximum value: 31536000
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 500 **
multiple-guest-add	Enable/disable addition of multiple guests.	option	-

Option	Description
disable	Enable setting.
enable	Disable setting.

** Values may differ between models.

config match

Parameter	Description	Type	Size
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
user-id	Guest ID.	string	Maximum length: 64
name	Guest name.	string	Maximum length: 64

Parameter	Description	Type	Size
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
description	Description.	string	Maximum length: 127

config rule

Parameter	Description	Type	Size
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

voip

This section includes syntax for the following commands:

- config voip profile on page 1142

config voip profile

Configure VoIP profiles.

```
config voip profile
   Description: Configure VoIP profiles.
   edit <name>
      set comment {var-string}
      config sip
         Description: SIP.
         set status [disable|enable]
         set rtp [disable|enable]
         set nat-port-range {user}
         set open-register-pinhole [disable|enable]
         set open-contact-pinhole [disable|enable]
         set strict-register [disable|enable]
         set register-rate {integer}
         set invite-rate {integer}
         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-pinhole [disable|enable]
         set open-record-route-pinhole [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 message-rate {integer}
```

```
set notify-rate {integer}
set refer-rate {integer}
set update-rate {integer}
set options-rate {integer}
set ack-rate {integer}
set prack-rate {integer}
set info-rate {integer}
set publish-rate {integer}
set bye-rate {integer}
set cancel-rate {integer}
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-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
comment	Comment.	var-string	Maximum length: 255

config sip

Parameter	Description	Type	Size
status	Enable/disable SIP.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
rtp	Enable/disable create pinholes for RTP traffic to traverse firewall.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
nat-port-range	RTP NAT port range.	user	Not Specified
open-register-pinhole	Enable/disable open pinhole for REGISTER Contact port.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable status. *enable* Enable status.		
open-contact-pinhole	Enable/disable open pinhole for non-REGISTER Contact port.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
strict-register	Enable/disable only allow the registrar to connect.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
register-rate	REGISTER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
invite-rate	INVITE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
max-dialogs	Maximum number of concurrent calls/dialogs (per policy).	integer	Minimum value: 0 Maximum value: 4294967295
max-line-length	Maximum SIP header line length .	integer	Minimum value: 78 Maximum value: 4096
block-long-lines	Enable/disable block requests with headers exceeding max-line-length.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-unknown	Block unrecognized SIP requests .	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
call-keepalive	Continue tracking calls with no RTP for this many minutes.	integer	Minimum value: 0 Maximum value: 10080
block-ack	Enable/disable block ACK requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-bye	Enable/disable block BYE requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-cancel	Enable/disable block CANCEL requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-info	Enable/disable block INFO requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-invite	Enable/disable block INVITE requests.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-message	Enable/disable block MESSAGE requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-notify	Enable/disable block NOTIFY requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-options	Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-prack	Enable/disable block prack requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-publish	Enable/disable block PUBLISH requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-refer	Enable/disable block REFER requests.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-register	Enable/disable block REGISTER requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-subscribe	Enable/disable block SUBSCRIBE requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
block-update	Enable/disable block UPDATE requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
register-contact-trace	Enable/disable trace original IP/port within the contact header of REGISTER requests.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
open-via-pinhole	Enable/disable open pinhole for Via port.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
open-record-route-pinhole	Enable/disable open pinhole for Record-Route port.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable status. *enable* Enable status.		
rfc2543-branch	Enable/disable support via branch compliant with RFC 2543.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
log-violations	Enable/disable logging of SIP violations.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
log-call-summary	Enable/disable logging of SIP call summary.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
nat-trace	Enable/disable preservation of original IP in SDP i line.	option	-
	Option **Description** *disable* Disable status. *enable* Enable status.		
subscribe-rate	SUBSCRIBE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
message-rate	MESSAGE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
notify-rate	NOTIFY request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
refer-rate	REFER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
update-rate	UPDATE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
options-rate	OPTIONS request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
ack-rate	ACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
prack-rate	PRACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
info-rate	INFO request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
publish-rate	PUBLISH request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
bye-rate	BYE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
cancel-rate	CANCEL request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
preserve-override	Override i line to preserve original IPS .	option	-

Option	Description
disable	Disable status.
enable	Enable status.

no-sdp-fixup	Enable/disable no SDP fix-up.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

contact-fixup	Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

max-idle-dialogs	Maximum number established but idle dialogs to retain (per policy).	integer	Minimum value: 0 Maximum value: 4294967295
block-geo-red-options	Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
hosted-nat-traversal	Hosted NAT Traversal (HNT).	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
hnt-restrict-source-ip	Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
max-body-length	Maximum SIP message body length (0 meaning no limit).	integer	Minimum value: 0 Maximum value: 4294967295
unknown-header	Action for unknown SIP header.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.
respond	Respond with error code.

Parameter	Description	Type	Size
malformed-request-line	Action for malformed request line.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.
respond	Respond with error code.

Parameter	Description	Type	Size
malformed-header-via	Action for malformed VIA header.	option	-

Option	Description
discard	Discard malformed messages.

Parameter	Description	Type	Size
	Option / **Description** *pass* — Bypass malformed messages. *respond* — Respond with error code.		
malformed-header-from	Action for malformed From header.	option	-
	Option / **Description** *discard* — Discard malformed messages. *pass* — Bypass malformed messages. *respond* — Respond with error code.		
malformed-header-to	Action for malformed To header.	option	-
	Option / **Description** *discard* — Discard malformed messages. *pass* — Bypass malformed messages. *respond* — Respond with error code.		
malformed-header-call-id	Action for malformed Call-ID header.	option	-
	Option / **Description** *discard* — Discard malformed messages. *pass* — Bypass malformed messages. *respond* — Respond with error code.		
malformed-header-cseq	Action for malformed CSeq header.	option	-
	Option / **Description** *discard* — Discard malformed messages. *pass* — Bypass malformed messages. *respond* — Respond with error code.		
malformed-header-rack	Action for malformed RAck header.	option	-

Parameter	Description	Type	Size
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-rseq	Action for malformed RSeq header.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-contact	Action for malformed Contact header.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-record-route	Action for malformed Record-Route header.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-route	Action for malformed Route header.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-expires	Action for malformed Expires header.	option	-

Parameter	Description	Type	Size
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-content-type	Action for malformed Content-Type header.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-content-length	Action for malformed Content-Length header.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-max-forwards	Action for malformed Max-Forwards header.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-allow	Action for malformed Allow header.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		

Parameter	Description	Type	Size
malformed-header-p-asserted-identity	Action for malformed P-Asserted-Identity header.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.
respond	Respond with error code.

Parameter	Description	Type	Size
malformed-header-sdp-v	Action for malformed SDP v line.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.
respond	Respond with error code.

Parameter	Description	Type	Size
malformed-header-sdp-o	Action for malformed SDP o line.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.
respond	Respond with error code.

Parameter	Description	Type	Size
malformed-header-sdp-s	Action for malformed SDP s line.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.
respond	Respond with error code.

Parameter	Description	Type	Size
malformed-header-sdp-i	Action for malformed SDP i line.	option	-

Option	Description
discard	Discard malformed messages.
pass	Bypass malformed messages.

Parameter	Description	Type	Size
	Option **Description** *respond* Respond with error code.		
malformed-header-sdp-c	Action for malformed SDP c line.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-sdp-b	Action for malformed SDP b line.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-sdp-z	Action for malformed SDP z line.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-sdp-k	Action for malformed SDP k line.	option	-
	Option **Description** *discard* Discard malformed messages. *pass* Bypass malformed messages. *respond* Respond with error code.		
malformed-header-sdp-a	Action for malformed SDP a line.	option	-

Parameter	Description	Type	Size
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-sdp-t	Action for malformed SDP t line.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-sdp-r	Action for malformed SDP r line.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
malformed-header-sdp-m	Action for malformed SDP m line.	option	-
	Option / **Description** *discard* / Discard malformed messages. *pass* / Bypass malformed messages. *respond* / Respond with error code.		
provisional-invite-expiry-time	Expiry time for provisional INVITE .	integer	Minimum value: 10 Maximum value: 3600
ips-rtp	Enable/disable allow IPS on RTP.	option	-
	Option / **Description** *disable* / Disable status. *enable* / Enable status.		
ssl-mode	SSL/TLS mode for encryption & decryption of traffic.	option	-

Parameter	Description	Type	Size
	Option / **Description** *off* — No SSL. *full* — 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	-
	Option / **Description** *enable* — Send empty fragments. *disable* — Do not send empty fragments.		
ssl-client-renegotiation	Allow/block client renegotiation by server.	option	-
	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-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-
	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-pfs	SSL Perfect Forward Secrecy.	option	-
	Option / **Description** *require* — PFS mandatory. *deny* — PFS rejected. *allow* — PFS allowed.		
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-
	Option / **Description** *ssl-3.0* — SSL 3.0.		

Parameter	Description	Type	Size
	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 to negotiate.	option	-
	Option / **Description** *ssl-3.0* / SSL 3.0. *tls-1.0* / TLS 1.0. *tls-1.1* / TLS 1.1. *tls-1.2* / TLS 1.2. *tls-1.3* / TLS 1.3.		
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
status	Enable/disable SCCP.	option	-
	Option / **Description** *disable* / Disable status. *enable* / Enable status.		
block-mcast	Enable/disable block multicast RTP connections.	option	-
	Option / **Description** *disable* / Disable status. *enable* / Enable status.		

Parameter	Description	Type	Size
verify-header	Enable/disable verify SCCP header content.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
log-call-summary	Enable/disable log summary of SCCP calls.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
log-violations	Enable/disable logging of SCCP violations.	option	-

Option	Description
disable	Disable status.
enable	Enable status.

Parameter	Description	Type	Size
max-calls	Maximum calls per minute per SCCP client (max 65535).	integer	Minimum value: 0 Maximum value: 65535

vpn

This section includes syntax for the following commands:

- config vpn ssl web user-bookmark on page 1194
- config vpn certificate ocsp-server on page 1169
- config vpn ipsec manualkey-interface on page 1266
- config vpn pptp on page 1270
- config vpn certificate ca on page 1162
- config vpn certificate remote on page 1164
- config vpn ipsec phase1-interface on page 1236
- config vpn certificate local on page 1165
- config vpn status l2tp on page 1274
- config vpn ipsec tunnel details on page 1269
- config vpn ike gateway on page 1274
- config vpn l2tp on page 1270
- config vpn certificate crl on page 1167
- config vpn ssl settings on page 1198
- config vpn status ssl hw-acceleration-status on page 1275
- config vpn ipsec phase2-interface on page 1258
- config vpn ipsec phase1 on page 1210
- config vpn ipsec tunnel name on page 1269
- config vpn ipsec phase2 on page 1227
- config vpn ipsec stats crypto on page 1269
- config vpn ipsec tunnel summary on page 1269
- config vpn ssl web user-group-bookmark on page 1190
- config vpn ssl web host-check-software on page 1174
- config vpn ipsec forticlient on page 1268
- config vpn certificate setting on page 1170
- config vpn status ssl list on page 1274
- config vpn ssl monitor on page 1209
- config vpn ipsec manualkey on page 1234
- config vpn ssl web portal on page 1175
- config vpn ssl web realm on page 1173
- config vpn ipsec concentrator on page 1236
- config vpn ocvpn on page 1271
- config vpn ipsec stats tunnel on page 1269
- config vpn status pptp on page 1274

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
ca	CA certificate as a PEM file.	user	Not Specified
range	Either global or VDOM IP address range for the CA certificate.	option	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

Parameter	Description	Type	Size
source	CA certificate source type.	option	-

Option	Description
factory	Factory installed certificate.
user	User generated certificate.
bundle	Bundle file certificate.

Parameter	Description	Type	Size
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-

Option	Description
enable	Trusted CA for SSL inspection.
disable	Untrusted CA for SSL inspection.

Parameter	Description	Type	Size
scep-url	URL of the SCEP server.	string	Maximum length: 255

Parameter	Description	Type	Size
auto-update-days	Number of days to wait before requesting an updated CA certificate .	integer	Minimum value: 0 Maximum value: 4294967295
auto-update-days-warning	Number of days before an expiry-warning message is generated .	integer	Minimum value: 0 Maximum value: 4294967295
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified

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
remote	Remote certificate.	user	Not Specified
range	Either the global or VDOM IP address range for the remote certificate.	option	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

Parameter	Description	Type	Size
source	Remote certificate source type.	option	-

Option	Description
factory	Factory installed certificate.

Parameter	Description	Type	Size

Option	Description
user	User generated certificate.
bundle	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 [keyupate|renewal]
   next
end
```

config vpn certificate local

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
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	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

source	Certificate source type.	option	-

Option	Description
factory	Factory installed certificate.
user	User generated certificate.
bundle	Bundle file certificate.

auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295
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
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	-

Option	Description
printable	Printable encoding (default).
utf8	UTF-8 encoding.

Parameter	Description	Type	Size
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified
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	-

Option	Description
asn1dn	ASN.1 distinguished name.
fqdn	Fully qualified domain name.

Parameter	Description	Type	Size
enroll-protocol	Certificate enrollment protocol.	option	-

Option	Description
none	None (default).
scep	Simple Certificate Enrollment Protocol.
cmpv2	Certificate Management Protocol Version 2.

Parameter	Description	Type	Size
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	-

Option	Description
keyupate	Key Update.
renewal	Renewal.

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
crl	Certificate Revocation List as a PEM file.	user	Not Specified
range	Either global or VDOM IP address range for the certificate.	option	-

Option	Description
global	Global range.
vdom	VDOM IP address range.

Parameter	Description	Type	Size
source	Certificate source type.	option	-

Option	Description
factory	Factory installed certificate.
user	User generated certificate.
bundle	Bundle file certificate.

Parameter	Description	Type	Size
update-vdom	VDOM for CRL update.	string	Maximum length: 31
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

Parameter	Description	Type	Size
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
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified

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
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	-

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

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 cn-match [substring|value]
   set strict-crl-check [enable|disable]
   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
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-

Option	Description
certificate	Use URL from certificate.
server	Use URL from configured OCSP server.

Parameter	Description	Type	Size
ssl-ocsp-source-ip	Source IP address to use to communicate with the OCSP server.	ipv4-address	Not Specified
ocsp-default-server	Default OCSP server.	string	Maximum length: 35
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

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
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted .	option	-

Option	Description
enable	Enable verification of the user certificate.
disable	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	-

Option	Description
enable	Enable verification of the entire certificate chain.
disable	Disable verification of the entire certificate chain.

subject-match	When searching for a matching certificate, control how to find matches in the certificate subject name.	option	-

Option	Description
substring	Find a match if any string in the certificate subject name matches the name being searched for.
value	Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.

Parameter	Description	Type	Size
cn-match	When searching for a matching certificate, control how to find matches in the cn attribute of the certificate subject name.	option	-

Option	Description
substring	Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.
value	Find a match if the cn attribute value string is an exact match with the name being searched for.

Parameter	Description	Type	Size
strict-crl-check	Enable/disable strict mode CRL checking.	option	-

Option	Description
enable	Enable strict mode CRL checking.
disable	Disable strict mode CRL checking.

Parameter	Description	Type	Size
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-

Option	Description
enable	Enable strict mode OCSP checking.
disable	Disable strict mode OCSP checking.

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

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode .	option	-

Option	Description
enable	Enable saving extra certificates in CMP mode.
disable	Disable saving extra certificates in CMP mode.

Parameter	Description	Type	Size
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode . **Option** — **Description** *enable* — Enable server certificate key usage checking in CMP mode. *disable* — Disable server certificate key usage checking in CMP mode.	option	-
certname-rsa1024	1024 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-rsa2048	2048 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-rsa4096	4096 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-dsa2048	2048 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-ecdsa256	256 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-ecdsa384	384 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-ecdsa521	521 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-ed25519	253 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35
certname-ed448	456 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35

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}
   next
end
```

config vpn ssl web realm

Parameter	Description	Type	Size
max-concurrent-user	Maximum concurrent users .	integer	Minimum value: 0 Maximum value: 65535
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

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
os-type	OS type.	option	-

Option	Description
windows	Microsoft Windows operating system.
macos	Apple MacOS operating system.

Parameter	Description	Type	Size
type	Type.	option	-

Parameter	Description	Type	Size
	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
action	Action.	option	-
	Option **Description** *require* Require. *deny* Deny.		
type	Type.	option	-
	Option **Description** *file* File. *registry* Registry. *process* 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-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-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 additional-params {var-string}
            set listening-port {integer}
            set remote-port {integer}
            set show-status-window [enable|disable]
            set description {var-string}
            set server-layout [de-de-qwertz|en-gb-qwerty|...]
            set security [rdp|nla|...]
            set preconnection-id {integer}
            set preconnection-blob {var-string}
            set load-balancing-info {var-string}
            set port {integer}
            set logon-user {var-string}
            set logon-password {password}
            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
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set heading {string}
set redir-url {var-string}
set theme [blue|green|...]
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 transform-backward-slashes [enable|disable]
set use-sdwan [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
tunnel-mode	Enable/disable IPv4 SSL-VPN tunnel mode.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
ip-mode	Method by which users of this SSL-VPN tunnel obtain IP addresses.	option	-

Option	Description
range	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.
user-group	Use IP the addresses associated with individual users or user groups (usually from external auth servers).

Parameter	Description	Type	Size
auto-connect	Enable/disable automatic connect by client when system is up.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
keep-alive	Enable/disable automatic reconnect for FortiClient connections.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
save-password	Enable/disable FortiClient saving the user's password.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
service-restriction	Enable/disable tunnel service restriction.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
split-tunneling	Enable/disable IPv4 split tunneling.	option	-
	Option **Description** *enable* Enable setting. *disable* 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
dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified
dns-suffix	DNS suffix.	var-string	Maximum length: 253
wins-server1	IPv4 WINS server 1.	ipv4-address	Not Specified
wins-server2	IPv4 WINS server 1.	ipv4-address	Not Specified
ipv6-tunnel-mode	Enable/disable IPv6 SSL-VPN tunnel mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
ipv6-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string	Maximum length: 79
ipv6-exclusive-routing	Enable/disable all IPv6 traffic go through tunnel only.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
ipv6-service-restriction	Enable/disable IPv6 tunnel service restriction.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
ipv6-split-tunneling	Enable/disable IPv6 split tunneling.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — 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
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified
web-mode	Enable/disable SSL VPN web mode.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

display-bookmark	Enable to display the web portal bookmark widget.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

allow-user-access	Allow user access to SSL-VPN applications.	option	-

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.
citrix	CITRIX access.
portforward	Port Forward access.

Parameter	Description	Type	Size
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
display-connection-tools	Enable to display the web portal connection tools widget.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
display-history	Enable to display the web portal user login history widget.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
display-status	Enable to display the web portal status widget.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
heading	Web portal heading message.	string	Maximum length: 31
redir-url	Client login redirect URL.	var-string	Maximum length: 255
theme	Web portal color scheme.	option	-

Option	Description
blue	Light blue theme.
green	Green theme.
neutrino	Neutrino theme.
melongene	Melongene theme (eggplant color).
mariner	Mariner theme (dark blue color).

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

smbv1	smbv1	option	-

Option	Description
enable	enable
disable	disable

smb-min-version	SMB minimum client protocol version.	option	-

Option	Description
smbv1	SMB version 1.
smbv2	SMB version 2.
smbv3	SMB version 3.

smb-max-version	SMB maximum client protocol version.	option	-

Option	Description
smbv1	SMB version 1.
smbv2	SMB version 2.
smbv3	SMB version 3.

transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
use-sdwan	Use SD-WAN rules to get output interface.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
host-check	Type of host checking performed on endpoints.	option	-

Option	Description
none	No host checking.
av	AntiVirus software recognized by the Windows Security Center.
fw	Firewall software recognized by the Windows Security Center.
av-fw	AntiVirus and firewall software recognized by the Windows Security Center.
custom	Custom.

Parameter	Description	Type	Size
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
host-check-policy <name>	One or more policies to require the endpoint to have specific security software. Host check software list name.	string	Maximum length: 79
limit-user-logins	Enable to limit each user to one SSL-VPN session at a time.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
mac-addr-check	Enable/disable MAC address host checking.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
mac-addr-action	Client MAC address action.	option	-

Parameter	Description	Type	Size
	Option / **Description** *allow* — Allow connection when client MAC address is matched. *deny* — Deny connection when client MAC address is matched.		
os-check	Enable to let the FortiGate decide action based on client OS.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
forticlient-download	Enable/disable download option for FortiClient.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
forticlient-download-method	FortiClient download method.	option	-
	Option / **Description** *direct* — Download via direct link. *ssl-vpn* — Download via SSL-VPN.		
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — 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

Parameter	Description	Type	Size
skip-check-for-unsupported-os	Enable to skip host check if client OS does not support it.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
skip-check-for-browser	Enable to skip host check for browser support.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
hide-sso-credential	Enable to prevent SSO credential being sent to client.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

config bookmarks

Parameter	Description	Type	Size
apptype	Application type.	option	-

Option	Description
ftp	FTP.
rdp	RDP.
sftp	SFTP.
smb	SMB/CIFS.
ssh	SSH.
telnet	Telnet.
vnc	VNC.
web	HTTP/HTTPS.

url	URL parameter.	var-string	Maximum length: 128

Parameter	Description	Type	Size
host	Host name/IP parameter.	var-string	Maximum length: 128
folder	Network shared file folder parameter.	var-string	Maximum length: 128
additional-params	Additional parameters.	var-string	Maximum length: 128
listening-port	Listening port .	integer	Minimum value: 0 Maximum value: 65535
remote-port	Remote port .	integer	Minimum value: 0 Maximum value: 65535
show-status-window	Enable/disable showing of status window.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

description	Description.	var-string	Maximum length: 128
server-layout	Server side keyboard layout.	option	-

Option	Description
de-de-qwertz	German (qwertz).
en-gb-qwerty	Engligh (UK).
en-us-qwerty	English (US).
es-es-qwerty	Spanish.
fr-ca-qwerty	Canadian French (qwerty).
fr-fr-azerty	French (azerty).
fr-ch-qwertz	Swiss French (qwertz).
it-it-qwerty	Italian.
ja-jp-qwerty	Japanese.
pt-br-qwerty	Portuguese/Brazilian.

Parameter	Description	Type	Size
	Option / **Description** *sv-se-qwerty* — Swedish. *tr-tr-qwerty* — Turkish. *failsafe* — Unknown keyboard.		
security	Security mode for RDP connection.	option	-
	Option / **Description** *rdp* — Standard RDP encryption. *nla* — Network Level Authentication. *tls* — TLS encryption. *any* — Allow the server to choose the type of security.		
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 2147483648
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
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535
logon-user	Logon user.	var-string	Maximum length: 35
logon-password	Logon password.	password	Not Specified
sso	Single Sign-On.	option	-
	Option / **Description** *disable* — Disable SSO. *static* — Static SSO. *auto* — Auto SSO.		
sso-credential	Single sign-on credentials.	option	-

Parameter	Description	Type	Size
	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	-
	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
value	Value.	var-string	Maximum length: 63

config mac-addr-check-rule

Parameter	Description	Type	Size
mac-addr-mask	Client MAC address mask.	integer	Minimum value: 1 Maximum value: 48
mac-addr-list <addr>	Client MAC address list. Client MAC address.	mac-address	Not Specified

config os-check-list

Parameter	Description	Type	Size
action	OS check options.	option	-
	Option / **Description** *deny* — Deny all OS versions.		

Parameter	Description	Type	Size
	Option / **Description** *allow* — Allow any OS version. *check-up-to-date* — Verify OS is up-to-date.		
tolerance	OS patch level tolerance.	integer	Minimum value: 0 Maximum value: 65535
latest-patch-level	Latest OS patch level.	user	Not Specified

config split-dns

Parameter	Description	Type	Size
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
dns-server2	DNS server 2.	ipv4-address	Not Specified
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 additional-params {var-string}
            set listening-port {integer}
            set remote-port {integer}
            set show-status-window [enable|disable]
            set description {var-string}
            set server-layout [de-de-qwertz|en-gb-qwerty|...]
            set security [rdp|nla|...]
```

```
            set preconnection-id {integer}
            set preconnection-blob {var-string}
            set load-balancing-info {var-string}
            set port {integer}
            set logon-user {var-string}
            set logon-password {password}
            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
apptype	Application type.	option	-

Option	Description
ftp	FTP.
rdp	RDP.
sftp	SFTP.
smb	SMB/CIFS.
ssh	SSH.
telnet	Telnet.
vnc	VNC.
web	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
additional-params	Additional parameters.	var-string	Maximum length: 128

Parameter	Description	Type	Size
listening-port	Listening port .	integer	Minimum value: 0 Maximum value: 65535
remote-port	Remote port .	integer	Minimum value: 0 Maximum value: 65535
show-status-window	Enable/disable showing of status window.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

description	Description.	var-string	Maximum length: 128
server-layout	Server side keyboard layout.	option	-

Option	Description
de-de-qwertz	German (qwertz).
en-gb-qwerty	Engligh (UK).
en-us-qwerty	English (US).
es-es-qwerty	Spanish.
fr-ca-qwerty	Canadian French (qwerty).
fr-fr-azerty	French (azerty).
fr-ch-qwertz	Swiss French (qwertz).
it-it-qwerty	Italian.
ja-jp-qwerty	Japanese.
pt-br-qwerty	Portuguese/Brazilian.
sv-se-qwerty	Swedish.
tr-tr-qwerty	Turkish.
failsafe	Unknown keyboard.

security	Security mode for RDP connection.	option	-

Parameter	Description	Type	Size
	Option / **Description** *rdp* / Standard RDP encryption. *nla* / Network Level Authentication. *tls* / TLS encryption. *any* / Allow the server to choose the type of security.		
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 2147483648
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
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535
logon-user	Logon user.	var-string	Maximum length: 35
logon-password	Logon password.	password	Not Specified
sso	Single Sign-On.	option	-
	Option / **Description** *disable* / Disable SSO. *static* / Static SSO. *auto* / Auto SSO.		
sso-credential	Single sign-on credentials.	option	-
	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

Parameter	Description	Type	Size
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-

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
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 additional-params {var-string}
            set listening-port {integer}
            set remote-port {integer}
            set show-status-window [enable|disable]
            set description {var-string}
            set server-layout [de-de-qwertz|en-gb-qwerty|...]
            set security [rdp|nla|...]
            set preconnection-id {integer}
            set preconnection-blob {var-string}
            set load-balancing-info {var-string}
            set port {integer}
            set logon-user {var-string}
            set logon-password {password}
            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
custom-lang	Personal language.	string	Maximum length: 35

config bookmarks

Parameter	Description	Type	Size
apptype	Application type.	option	-

Option	Description
ftp	FTP.
rdp	RDP.
sftp	SFTP.
smb	SMB/CIFS.
ssh	SSH.
telnet	Telnet.
vnc	VNC.
web	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
additional-params	Additional parameters.	var-string	Maximum length: 128

Parameter	Description	Type	Size
listening-port	Listening port .	integer	Minimum value: 0 Maximum value: 65535
remote-port	Remote port .	integer	Minimum value: 0 Maximum value: 65535
show-status-window	Enable/disable showing of status window.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

description	Description.	var-string	Maximum length: 128
server-layout	Server side keyboard layout.	option	-

Option	Description
de-de-qwertz	German (qwertz).
en-gb-qwerty	Engligh (UK).
en-us-qwerty	English (US).
es-es-qwerty	Spanish.
fr-ca-qwerty	Canadian French (qwerty).
fr-fr-azerty	French (azerty).
fr-ch-qwertz	Swiss French (qwertz).
it-it-qwerty	Italian.
ja-jp-qwerty	Japanese.
pt-br-qwerty	Portuguese/Brazilian.
sv-se-qwerty	Swedish.
tr-tr-qwerty	Turkish.
failsafe	Unknown keyboard.

security	Security mode for RDP connection.	option	-

Parameter	Description	Type	Size
	Option / **Description** *rdp* — Standard RDP encryption. *nla* — Network Level Authentication. *tls* — TLS encryption. *any* — Allow the server to choose the type of security.		
preconnection-id	The numeric ID of the RDP source .	integer	Minimum value: 0 Maximum value: 2147483648
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
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535
logon-user	Logon user.	var-string	Maximum length: 35
logon-password	Logon password.	password	Not Specified
sso	Single Sign-On.	option	-
	Option / **Description** *disable* — Disable SSO. *static* — Static SSO. *auto* — Auto SSO.		
sso-credential	Single sign-on credentials.	option	-
	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

Parameter	Description	Type	Size
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-

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
value	Value.	var-string	Maximum length: 63

config vpn ssl settings

Configure SSL VPN.

```
config vpn ssl settings
   Description: Configure SSL VPN.
   set reqclientcert [enable|disable]
   set user-peer {string}
   set ssl-max-proto-ver [tls1-0|tls1-1|...]
   set ssl-min-proto-ver [tls1-0|tls1-1|...]
   set tlsv1-0 [enable|disable]
   set tlsv1-1 [enable|disable]
   set tlsv1-2 [enable|disable]
   set tlsv1-3 [enable|disable]
   set banned-cipher {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 route-source-interface [enable|disable]
    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 encode-2f-sequence [enable|disable]
end
```

config vpn ssl settings

Parameter	Description	Type	Size
reqclientcert	Enable to require client certificates for all SSL-VPN users.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
user-peer	Name of user peer.	string	Maximum length: 35
ssl-max-proto-ver	SSL maximum protocol version.	option	-

Option	Description
tls1-0	TLS version 1.0.
tls1-1	TLS version 1.1.
tls1-2	TLS version 1.2.
tls1-3	TLS version 1.3.

Parameter	Description	Type	Size
ssl-min-proto-ver	SSL minimum protocol version.	option	-

Option	Description
tls1-0	TLS version 1.0.
tls1-1	TLS version 1.1.
tls1-2	TLS version 1.2.
tls1-3	TLS version 1.3.

Parameter	Description	Type	Size
tlsv1-0	tlsv1-0	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
tlsv1-1	tlsv1-1	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
tlsv1-2	tlsv1-2	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
tlsv1-3	tlsv1-3	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
banned-cipher	Select one or more cipher technologies that cannot be used in SSL-VPN negotiations.	option	-

Option	Description
RSA	Ban the use of cipher suites using RSA key.
DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.
ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.
DSS	Ban the use of cipher suites using DSS authentication.
ECDSA	Ban the use of cipher suites using ECDSA authentication.
AES	Ban the use of cipher suites using either 128 or 256 bit AES.
AESGCM	Ban the use of cipher suites AES in Galois Counter Mode (GCM).
CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.
3DES	Ban the use of cipher suites using triple DES
SHA1	Ban the use of cipher suites using HMAC-SHA1.
SHA256	Ban the use of cipher suites using HMAC-SHA256.
SHA384	Ban the use of cipher suites using HMAC-SHA384.
STATIC	Ban the use of cipher suites using static keys.

Parameter	Description	Type	Size
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
https-redirect	Enable/disable redirect of port 80 to SSL-VPN port.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
ssl-client-renegotiation	Enable to allow client renegotiation by the server if the tunnel goes down.	option	-
	Option **Description** *disable* Abort any SSL connection that attempts to renegotiate. *enable* Allow a SSL client to renegotiate.		
force-two-factor-auth	Enable only PKI users with two-factor authentication for SSL-VPNs.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
servercert	Name of the server certificate to be used for SSL-VPNs.	string	Maximum length: 35

Parameter	Description	Type	Size
algorithm	Force the SSL-VPN security level. High allows only high. Medium allows medium and high. Low allows any.	option	-

Option	Description
high	High algorithms.
medium	High and medium algorithms.
default	default
low	All algorithms.

idle-timeout	SSL VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200
auth-timeout	SSL-VPN authentication timeout .	integer	Minimum value: 0 Maximum value: 259200
login-attempt-limit	SSL VPN maximum login attempt times before block .	integer	Minimum value: 0 Maximum value: 4294967295
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
login-timeout	SSLVPN maximum login timeout .	integer	Minimum value: 10 Maximum value: 180
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout .	integer	Minimum value: 10 Maximum value: 60
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.	string	Maximum length: 79

Parameter	Description	Type	Size
	Address name.		
dns-suffix	DNS suffix used for SSL-VPN clients.	var-string	Maximum length: 253
dns-server1	DNS server 1.	ipv4-address	Not Specified
dns-server2	DNS server 2.	ipv4-address	Not Specified
wins-server1	WINS server 1.	ipv4-address	Not Specified
wins-server2	WINS server 2.	ipv4-address	Not Specified
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
route-source-interface	Enable to allow SSL-VPN sessions to bypass routing and bind to the incoming interface.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
url-obscuration	Enable to obscure the host name of the URL of the web browser display.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
http-compression	Enable to allow HTTP compression over SSL-VPN tunnels.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
http-only-cookie	Enable/disable SSL-VPN support for HttpOnly cookies.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
deflate-compression-level	Compression level (0~9).	integer	Minimum value: 0 Maximum value: 9
deflate-min-data-size	Minimum amount of data that triggers compression .	integer	Minimum value: 200 Maximum value: 65535
port	SSL-VPN access port .	integer	Minimum value: 1 Maximum value: 65535
port-precedence	Enable means that if SSL-VPN connections are allowed on an interface admin GUI connections are blocked on that interface.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
auto-tunnel-static-route	Enable to auto-create static routes for the SSL-VPN tunnel IP addresses.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-
	Option / **Description** *pass* / Forward the same HTTP header. *add* / Add the HTTP header. *remove* / Remove the HTTP header.		

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

default-portal	Default SSL VPN portal.	string	Maximum length: 35
dtls-tunnel	Enable DTLS to prevent eavesdropping, tampering, or message forgery.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

dtls-max-proto-ver	DTLS maximum protocol version.	option	-

Option	Description
dtls1-0	DTLS version 1.0.
dtls1-2	DTLS version 1.2.

dtls-min-proto-ver	DTLS minimum protocol version.	option	-

Parameter	Description	Type	Size
	Option / **Description** *dtls1-0* / DTLS version 1.0. *dtls1-2* / DTLS version 1.2.		
check-referer	Enable/disable verification of referer field in HTTP request header.	option	-
	Option / **Description** *enable* / Enable verification of referer field in HTTP request header. *disable* / 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
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
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-
	Option / **Description** *enable* / Enable checking of source IP for authentication session. *disable* / Disable checking of source IP for authentication session.		
tunnel-connect-without-reauth	Enable/disable tunnel connection without re-authorization if previous connection dropped.	option	-
	Option / **Description** *enable* / Enable tunnel connection without re-authorization. *disable* / Disable tunnel connection without re-authorization.		
tunnel-user-session-timeout	Time out value to clean up user session after tunnel connection is dropped .	integer	Minimum value: 1 Maximum value: 255
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
encode-2f-sequence	Encode \2F sequence to forward slash in URLs.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		

config authentication-rule

Parameter	Description	Type	Size
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	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
users <name>	User name. User name.	string	Maximum length: 79

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable setting.
disable	Disable setting.

user-peer	Name of user peer.	string	Maximum length: 35
cipher	SSL VPN cipher strength.	option	-

Option	Description
any	Any cipher strength.
high	High cipher strength (>= 168 bits).
medium	Medium cipher strength (>= 128 bits).

auth	SSL VPN authentication method restriction.	option	-

Option	Description
any	Any
local	Local
radius	RADIUS
tacacs+	TACACS+
ldap	LDAP

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 usrgrp {string}
      set peer {string}
      set peergrp {string}
      set mode-cfg [disable|enable]
      set assign-ip [disable|enable]
      set assign-ip-from [range|usrgrp|...]
      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 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 authusrgrp {string}
set mesh-selector-type [disable|subnet|...]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ha-sync-esp-seqno [enable|disable]
set nattraversal [enable|disable|...]
```

```
      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-redundant {integer}
      set fec-ingress [enable|disable]
      set fec-receive-timeout {integer}
      set network-overlay [disable|enable]
      set network-id {integer}
   next
end
```

config vpn ipsec phase1

Parameter	Description	Type	Size
type	Remote gateway type.	option	-

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	-

Option	Description
1	Use IKEv1 protocol.
2	Use IKEv2 protocol.

remote-gw	Remote VPN gateway.	ipv4-address	Not Specified
local-gw	Local VPN gateway.	ipv4-address	Not Specified
remotegw-ddns	Domain name of remote gateway (eg. name.DDNS.com).	string	Maximum length: 63

Parameter	Description	Type	Size
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800
certificate <name>	Names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79
authmethod	Authentication method.	option	-

Option	Description
psk	PSK authentication method.
signature	Signature authentication method.

Parameter	Description	Type	Size
authmethod-remote	Authentication method (remote side).	option	-

Option	Description
psk	PSK authentication method.
signature	Signature authentication method.

Parameter	Description	Type	Size
mode	ID protection mode used to establish a secure channel.	option	-

Option	Description
aggressive	Aggressive mode.
main	Main mode.

Parameter	Description	Type	Size
peertype	Accept this peer type.	option	-

Option	Description
any	Accept any peer ID.
one	Accept this peer ID.
dialup	Accept peer ID in dialup group.
peer	Accept this peer certificate.
peergrp	Accept this peer certificate group.

Parameter	Description	Type	Size
peerid	Accept this peer identity.	string	Maximum length: 255
usrgrp	User group name for dialup peers.	string	Maximum length: 35

Parameter	Description	Type	Size
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	-

Option	Description
disable	Disable Configuration Method.
enable	Enable Configuration Method.

assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-

Option	Description
disable	Do not assign an IP address to the IPsec interface.
enable	Assign an IP address to the IPsec interface.

assign-ip-from	Method by which the IP address will be assigned.	option	-

Option	Description
range	Assign IP address from locally defined range.
usrgrp	Assign IP address via user group.
dhcp	Assign IP address via DHCP.
name	Assign IP address from firewall address or group.

ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified
dns-mode	DNS server mode.	option	-

Option	Description
manual	Manually configure DNS servers.
auto	Use default DNS servers.

Parameter	Description	Type	Size
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified
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
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
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-

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
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-

Option	Description
disable	Disable local LAN access on Unity clients.
enable	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	-

Option	Description
disable	Disable saving XAuth username and password on VPN clients.
enable	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	-

Option	Description
disable	Disable allowing the VPN client to bring up the tunnel when there is no traffic.
enable	Enable allowing the VPN client to bring up the tunnel when there is no traffic.

client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-

Option	Description
disable	Disable allowing the VPN client to keep the tunnel up when there is no traffic.
enable	Enable allowing the VPN client to keep the tunnel up when there is no traffic.

backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79
proposal	Phase1 proposal.	option	-

Parameter	Description	Type	Size

Option	Description
des-md5	des-md5
des-sha1	des-sha1
des-sha256	des-sha256
des-sha384	des-sha384
des-sha512	des-sha512
3des-md5	3des-md5
3des-sha1	3des-sha1
3des-sha256	3des-sha256
3des-sha384	3des-sha384
3des-sha512	3des-sha512
aes128-md5	aes128-md5
aes128-sha1	aes128-sha1
aes128-sha256	aes128-sha256
aes128-sha384	aes128-sha384
aes128-sha512	aes128-sha512
aes128gcm-prfsha1	aes128gcm-prfsha1
aes128gcm-prfsha256	aes128gcm-prfsha256
aes128gcm-prfsha384	aes128gcm-prfsha384
aes128gcm-prfsha512	aes128gcm-prfsha512
aes192-md5	aes192-md5
aes192-sha1	aes192-sha1
aes192-sha256	aes192-sha256
aes192-sha384	aes192-sha384
aes192-sha512	aes192-sha512
aes256-md5	aes256-md5
aes256-sha1	aes256-sha1
aes256-sha256	aes256-sha256
aes256-sha384	aes256-sha384
aes256-sha512	aes256-sha512

Parameter	Description	Type	Size
	Option **Description** *aes256gcm-prfsha1* aes256gcm-prfsha1 *aes256gcm-prfsha256* aes256gcm-prfsha256 *aes256gcm-prfsha384* aes256gcm-prfsha384 *aes256gcm-prfsha512* aes256gcm-prfsha512 *chacha20poly1305-prfsha1* chacha20poly1305-prfsha1 *chacha20poly1305-prfsha256* chacha20poly1305-prfsha256 *chacha20poly1305-prfsha384* chacha20poly1305-prfsha384 *chacha20poly1305-prfsha512* chacha20poly1305-prfsha512		
add-route	Enable/disable control addition of a route to peer destination selector.	option	-
	Option **Description** *disable* Do not add a route to destination of peer selector. *enable* Add route to destination of peer selector.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-
	Option **Description** *enable* Automatically add a route to the remote gateway. *disable* 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
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255

Parameter	Description	Type	Size
priority	Priority for routes added by IKE .	integer	Minimum value: 0 Maximum value: 4294967295
localid	Local ID.	string	Maximum length: 63
localid-type	Local ID type.	option	-

Option	Description
auto	Select ID type automatically.
fqdn	Use fully qualified domain name.
user-fqdn	Use user fully qualified domain name.
keyid	Use key-id string.
address	Use local IP address.
asn1dn	Use ASN.1 distinguished name.

auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-

Option	Description
enable	Enable automatic initiation of IKE SA negotiation.
disable	Disable automatic initiation of IKE SA negotiation.

negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-

Option	Description
enable	Enable intra-IKE fragmentation support on re-transmission.
disable	Disable intra-IKE fragmentation support.

dpd	Dead Peer Detection mode.	option	-

Option	Description
disable	Disable Dead Peer Detection.

Parameter	Description	Type	Size
	Option / **Description** *on-idle* — Trigger Dead Peer Detection when IPsec is idle. *on-demand* — Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.		
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10
dpd-retryinterval	DPD retry interval.	user	Not Specified
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-
	Option / **Description** *enable* — Enable FortiClient enforcement. *disable* — Disable FortiClient enforcement.		
comments	Comment.	var-string	Maximum length: 255
npu-offload *	Enable/disable offloading NPU.	option	-
	Option / **Description** *enable* — Enable NPU offloading. *disable* — Disable NPU offloading.		
send-cert-chain	Enable/disable sending certificate chain.	option	-
	Option / **Description** *enable* — Enable sending certificate chain. *disable* — Disable sending certificate chain.		
dhgrp	DH group.	option	-
	Option / **Description** *1* — DH Group 1. *2* — DH Group 2. *5* — DH Group 5. *14* — DH Group 14.		

Parameter	Description	Type	Size
	Option **Description** *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.		
suite-b	Use Suite-B.	option	-
	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	-
	Option **Description** *enable* Enable IKEv2 EAP authentication. *disable* Disable IKEv2 EAP authentication.		
eap-identity	IKEv2 EAP peer identity type.	option	-
	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

Parameter	Description	Type	Size
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-

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	-

Option	Description
disable	Disable use of IKEv2 Postquantum Preshared Key (PPK).
allow	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).
require	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	-

Option	Description
custom	Custom VPN configuration.
dialup-forticlient	Dial Up - FortiClient Windows, Mac and Android.
dialup-ios	Dial Up - iPhone / iPad Native IPsec Client.
dialup-android	Dial Up - Android Native IPsec Client.
dialup-windows	Dial Up - Windows Native IPsec Client.
dialup-cisco	Dial Up - Cisco IPsec Client.
static-fortigate	Site to Site - FortiGate.
dialup-fortigate	Dial Up - FortiGate.
static-cisco	Site to Site - Cisco.
dialup-cisco-fw	Dialup Up - Cisco Firewall.
simplified-static-fortigate	Site to Site - FortiGate (SD-WAN).

Parameter	Description	Type	Size
	Option / **Description** *hub-fortigate-auto-discovery* — Hub role in a Hub-and-Spoke auto-discovery VPN. *spoke-fortigate-auto-discovery* — Spoke role in a Hub-and-Spoke auto-discovery VPN.		
xauthtype	XAuth type.	option	-
	Option / **Description** *disable* — Disable. *client* — Enable as client. *pap* — Enable as server PAP. *chap* — Enable as server CHAP. *auto* — Enable as server auto.		
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-
	Option / **Description** *disable* — Disable IKE SA re-authentication. *enable* — 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	-
	Option / **Description** *enable* — Enable IKEv2 IDi group authentication. *disable* — 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
authusrgrp	Authentication user group.	string	Maximum length: 35
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable. *subnet* / Enable addition of matching subnet selector. *host* / Enable addition of host to host selector.		
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-
	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
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-
	Option / **Description** *enable* / Enable HA syncing of ESP sequence numbers. *disable* / Disable HA syncing of ESP sequence numbers.		
nattraversal	Enable/disable NAT traversal.	option	-
	Option / **Description** *enable* / Enable IPsec NAT traversal. *disable* / Disable IPsec NAT traversal. *forced* / Force IPsec NAT traversal on.		
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-
	Option / **Description** *enable* / Enable childless IKEv2 initiation (RFC 6023). *disable* / Disable childless IKEv2 initiation (RFC 6023).		

Parameter	Description	Type	Size
rekey	Enable/disable phase1 rekey.	option	-

Option	Description
enable	Enable phase1 rekey.
disable	Disable phase1 rekey.

Parameter	Description	Type	Size
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-

Option	Description
enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).
disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).

Parameter	Description	Type	Size
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-

Option	Description
sha1	SHA1.
sha2-256	SHA2-256.
sha2-384	SHA2-384.
sha2-512	SHA2-512.

Parameter	Description	Type	Size
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-

Option	Description
pkcs1	RSASSA PKCS#1 v1.5.
pss	RSASSA Probabilistic Signature Scheme (PSS).

Parameter	Description	Type	Size
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-

Option	Description
disable	Disable peer ID uniqueness enforcement.
keep-new	Enforce peer ID uniqueness, keep new connection if collision found.
keep-old	Enforce peer ID uniqueness, keep old connection if collision found.

Parameter	Description	Type	Size
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-

Parameter	Description	Type	Size
	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	-
	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
fec-base	Number of base Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100
fec-redundant	Number of redundant Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-
	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
network-overlay	Enable/disable network overlays.	option	-
	Option / **Description** *disable* — Disable network overlays.		

Parameter	Description	Type	Size
	Option: *enable* — Description: Enable network overlays.		
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified

config ipv6-exclude-range

Parameter	Description	Type	Size
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 keylifekbs {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 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
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 35
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
use-natip	Enable to use the FortiGate public IP as the source selector when outbound NAT is used.	option	-

Option	Description
enable	Replace source selector with interface IP when using outbound NAT.
disable	Do not modify source selector when using outbound NAT.

Parameter	Description	Type	Size
selector-match	Match type to use when comparing selectors.	option	-

Parameter	Description	Type	Size

Option	Description
exact	Match selectors exactly.
subset	Match selectors by subset.
auto	Use subset or exact match depending on selector address type.

proposal	Phase2 proposal.	option	-

Option	Description
null-md5	null-md5
null-sha1	null-sha1
null-sha256	null-sha256
null-sha384	null-sha384
null-sha512	null-sha512
des-null	des-null
des-md5	des-md5
des-sha1	des-sha1
des-sha256	des-sha256
des-sha384	des-sha384
des-sha512	des-sha512
3des-null	3des-null
3des-md5	3des-md5
3des-sha1	3des-sha1
3des-sha256	3des-sha256
3des-sha384	3des-sha384
3des-sha512	3des-sha512
aes128-null	aes128-null
aes128-md5	aes128-md5
aes128-sha1	aes128-sha1
aes128-sha256	aes128-sha256
aes128-sha384	aes128-sha384
aes128-sha512	aes128-sha512

Parameter	Description	Type	Size
	Option / **Description** *aes128gcm* / aes128gcm *aes192-null* / aes192-null *aes192-md5* / aes192-md5 *aes192-sha1* / aes192-sha1 *aes192-sha256* / aes192-sha256 *aes192-sha384* / aes192-sha384 *aes192-sha512* / aes192-sha512 *aes256-null* / aes256-null *aes256-md5* / aes256-md5 *aes256-sha1* / aes256-sha1 *aes256-sha256* / aes256-sha256 *aes256-sha384* / aes256-sha384 *aes256-sha512* / aes256-sha512 *aes256gcm* / aes256gcm *chacha20poly1305* / chacha20poly1305		
pfs	Enable/disable PFS feature.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-
	Option / **Description** *enable* / Set IPv4 DF. *disable* / Reset IPv4 DF.		
dhgrp	Phase2 DH group.	option	-
	Option / **Description** *1* / DH Group 1. *2* / DH Group 2.		

Parameter	Description	Type	Size
	Option **Description** *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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
keepalive	Enable/disable keep alive.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
add-route	Enable/disable automatic route addition.	option	-

Parameter	Description	Type	Size
	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.		
keylifeseconds	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800
keylifekbs	Phase2 key life in number of bytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295
keylife-type	Keylife type.	option	-
	Option **Description** *seconds* Key life in seconds. *kbs* Key life in kilobytes. *both* Key life both.		
single-source	Enable/disable single source IP restriction.	option	-
	Option **Description** *enable* Only single source IP will be accepted. *disable* Source IP range will be accepted.		
route-overlap	Action for overlapping routes.	option	-
	Option **Description** *use-old* Use the old route and do not add the new route. *use-new* Delete the old route and add the new route. *allow* Allow overlapping routes.		
encapsulation	ESP encapsulation mode.	option	-
	Option **Description** *tunnel-mode* Use tunnel mode encapsulation. *transport-mode* Use transport mode encapsulation.		

Parameter	Description	Type	Size
l2tp	Enable/disable L2TP over IPsec.	option	-
	Option / **Description** *enable* — Enable L2TP over IPsec. *disable* — Disable L2TP over IPsec.		
comments	Comment.	var-string	Maximum length: 255
protocol	Quick mode protocol selector .	integer	Minimum value: 0 Maximum value: 255
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	-
	Option / **Description** *subnet* — IPv4 subnet. *range* — IPv4 range. *ip* — IPv4 IP. *name* — IPv4 firewall address or group name.		
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
src-port	Quick mode source port .	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
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	-

Option	Description
subnet	IPv4 subnet.
range	IPv4 range.
ip	IPv4 IP.
name	IPv4 firewall address or group name.

dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified
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
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
dst-port	Quick mode destination port .	integer	Minimum value: 0 Maximum value: 65535

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 remotespi {user}
      set npu-offload [enable|disable]
```

```
    next
end
```

config vpn ipsec manualkey

Parameter	Description	Type	Size
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15
remote-gw	Peer gateway.	ipv4-address	Not Specified
local-gw	Local gateway.	ipv4-address-any	Not Specified
authentication	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-

Option	Description
null	Null.
md5	MD5.
sha1	SHA1.
sha256	SHA256.
sha384	SHA384.
sha512	SHA512.

encryption	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-

Option	Description
null	Null.
des	DES.
3des	3DES.
aes128	AES128.
aes192	AES192.
aes256	AES256.

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

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable NPU offloading.
disable	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 <name>
      set src-check [disable|enable]
      set member <name1>, <name2>, ...
   next
end
```

config vpn ipsec concentrator

Parameter	Description	Type	Size
src-check	Enable to check source address of phase 2 selector. Disable to check only the destination selector.	option	-

Option	Description
disable	Ignore source selector when choosing tunnel.
enable	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 usrgrp {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 tunnel-search [selectors|nexthop]
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 mode-cfg [disable|enable]
set assign-ip [disable|enable]
set assign-ip-from [range|usrgrp|...]
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 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 authusrgrp {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 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 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-redundant {integer}
    set fec-ingress [enable|disable]
    set fec-receive-timeout {integer}
    set network-overlay [disable|enable]
    set network-id {integer}
  next
end
```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size
type	Remote gateway type.	option	-

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.

Parameter	Description	Type	Size
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35
ip-version	IP version to use for VPN interface.	option	-

Option	Description
4	Use IPv4 addressing for gateways.
6	Use IPv6 addressing for gateways.

ike-version	IKE protocol version.	option	-

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
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
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
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79
authmethod	Authentication method.	option	-

Option	Description
psk	PSK authentication method.
signature	Signature authentication method.

authmethod-remote	Authentication method (remote side).	option	-

Parameter	Description	Type	Size
	Option / **Description** *psk* — PSK authentication method. *signature* — Signature authentication method.		
mode	The ID protection mode used to establish a secure channel.	option	-
	Option / **Description** *aggressive* — Aggressive mode. *main* — Main mode.		
peertype	Accept this peer type.	option	-
	Option / **Description** *any* — Accept any peer ID. *one* — Accept this peer ID. *dialup* — Accept peer ID in dialup group. *peer* — Accept this peer certificate. *peergrp* — 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
default-gw-priority	Priority for default gateway route. A higher priority number signifies a less preferred route.	integer	Minimum value: 0 Maximum value: 4294967295
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
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	-

Parameter	Description	Type	Size
	Option / **Description** *immediate* — Fail back immediately after primary recovers. *delay* — Number of seconds to delay fail back after primary recovers. *time* — 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
monitor-hold-down-weekday	Day of the week to recover once primary re-establishes.	option	-
	Option / **Description** *everyday* — Every Day. *sunday* — Sunday. *monday* — Monday. *tuesday* — Tuesday. *wednesday* — Wednesday. *thursday* — Thursday. *friday* — Friday. *saturday* — 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	-
	Option / **Description** *enable* — Create a kernel device for every tunnel. *disable* — Do not create a kernel device for tunnels.		
tunnel-search	Tunnel search method for when the interface is shared.	option	-
	Option / **Description** *selectors* — Search for tunnel in selectors. *nexthop* — Search for tunnel using nexthop.		

Parameter	Description	Type	Size
passive-mode	Enable/disable IPsec passive mode for static tunnels.	option	-

Option	Description
enable	Enable IPsec passive mode.
disable	Disable IPsec passive mode.

Parameter	Description	Type	Size
exchange-interface-ip	Enable/disable exchange of IPsec interface IP address.	option	-

Option	Description
enable	Enable exchange of IPsec interface IP address.
disable	Disable exchange of IPsec interface IP address.

Parameter	Description	Type	Size
exchange-ip-addr4	IPv4 address to exchange with peers.	ipv4-address	Not Specified
exchange-ip-addr6	IPv6 address to exchange with peers	ipv6-address	Not Specified
aggregate-member	Enable/disable use as an aggregate member.	option	-

Option	Description
enable	Enable use as an aggregate member.
disable	Disable use as an aggregate member.

Parameter	Description	Type	Size
mode-cfg	Enable/disable configuration method.	option	-

Option	Description
disable	Disable Configuration Method.
enable	Enable Configuration Method.

Parameter	Description	Type	Size
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-

Option	Description
disable	Do not assign an IP address to the IPsec interface.
enable	Assign an IP address to the IPsec interface.

Parameter	Description	Type	Size
assign-ip-from	Method by which the IP address will be assigned.	option	-

Parameter	Description	Type	Size
	Option **Description** *range* Assign IP address from locally defined range. *usrgrp* Assign IP address via user group. *dhcp* Assign IP address via DHCP. *name* Assign IP address from firewall address or group.		
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified
dns-mode	DNS server mode.	option	-
	Option **Description** *manual* Manually configure DNS servers. *auto* Use default DNS servers.		
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified
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

Parameter	Description	Type	Size
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 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
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-

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	-

Option	Description
disable	Disable local LAN access on Unity clients.
enable	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	-

Option	Description
disable	Disable saving XAuth username and password on VPN clients.
enable	Enable saving XAuth username and password on VPN clients.

Parameter	Description	Type	Size
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-

Option	Description
disable	Disable allowing the VPN client to bring up the tunnel when there is no traffic.
enable	Enable allowing the VPN client to bring up the tunnel when there is no traffic.

client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-

Option	Description
disable	Disable allowing the VPN client to keep the tunnel up when there is no traffic.
enable	Enable allowing the VPN client to keep the tunnel up when there is no traffic.

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
des-md5	des-md5
des-sha1	des-sha1
des-sha256	des-sha256
des-sha384	des-sha384
des-sha512	des-sha512
3des-md5	3des-md5
3des-sha1	3des-sha1
3des-sha256	3des-sha256
3des-sha384	3des-sha384
3des-sha512	3des-sha512
aes128-md5	aes128-md5
aes128-sha1	aes128-sha1

Parameter	Description	Type	Size
	Option — **Description** *aes128-sha256* — aes128-sha256 *aes128-sha384* — aes128-sha384 *aes128-sha512* — aes128-sha512 *aes128gcm-prfsha1* — aes128gcm-prfsha1 *aes128gcm-prfsha256* — aes128gcm-prfsha256 *aes128gcm-prfsha384* — aes128gcm-prfsha384 *aes128gcm-prfsha512* — aes128gcm-prfsha512 *aes192-md5* — aes192-md5 *aes192-sha1* — aes192-sha1 *aes192-sha256* — aes192-sha256 *aes192-sha384* — aes192-sha384 *aes192-sha512* — aes192-sha512 *aes256-md5* — aes256-md5 *aes256-sha1* — aes256-sha1 *aes256-sha256* — aes256-sha256 *aes256-sha384* — aes256-sha384 *aes256-sha512* — aes256-sha512 *aes256gcm-prfsha1* — aes256gcm-prfsha1 *aes256gcm-prfsha256* — aes256gcm-prfsha256 *aes256gcm-prfsha384* — aes256gcm-prfsha384 *aes256gcm-prfsha512* — aes256gcm-prfsha512 *chacha20poly1305-prfsha1* — chacha20poly1305-prfsha1 *chacha20poly1305-prfsha256* — chacha20poly1305-prfsha256 *chacha20poly1305-prfsha384* — chacha20poly1305-prfsha384 *chacha20poly1305-prfsha512* — chacha20poly1305-prfsha512		
add-route	Enable/disable control addition of a route to peer destination selector.	option	-

Parameter	Description	Type	Size
	Option / **Description** *disable* — Do not add a route to destination of peer selector. *enable* — Add route to destination of peer selector.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-
	Option / **Description** *enable* — Automatically add a route to the remote gateway. *disable* — 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
distance	Distance for routes added by IKE .	integer	Minimum value: 1 Maximum value: 255
priority	Priority for routes added by IKE .	integer	Minimum value: 0 Maximum value: 4294967295
localid	Local ID.	string	Maximum length: 63
localid-type	Local ID type.	option	-
	Option / **Description** *auto* — Select ID type automatically. *fqdn* — Use fully qualified domain name. *user-fqdn* — Use user fully qualified domain name.		

Parameter	Description	Type	Size
	Option / **Description** *keyid* — Use key-id string. *address* — Use local IP address. *asn1dn* — Use ASN.1 distinguished name.		
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-
	Option / **Description** *enable* — Enable automatic initiation of IKE SA negotiation. *disable* — Disable automatic initiation of IKE SA negotiation.		
negotiate-timeout	IKE SA negotiation timeout in seconds .	integer	Minimum value: 1 Maximum value: 300
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-
	Option / **Description** *enable* — Enable intra-IKE fragmentation support on re-transmission. *disable* — Disable intra-IKE fragmentation support.		
ip-fragmentation	Determine whether IP packets are fragmented before or after IPsec encapsulation.	option	-
	Option / **Description** *pre-encapsulation* — Fragment before IPsec encapsulation. *post-encapsulation* — Fragment after IPsec encapsulation (RFC compliant).		
dpd	Dead Peer Detection mode.	option	-
	Option / **Description** *disable* — Disable Dead Peer Detection. *on-idle* — Trigger Dead Peer Detection when IPsec is idle. *on-demand* — Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.		

Parameter	Description	Type	Size
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10
dpd-retryinterval	DPD retry interval.	user	Not Specified
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-

Option	Description
enable	Enable FortiClient enforcement.
disable	Disable FortiClient enforcement.

comments	Comment.	var-string	Maximum length: 255
npu-offload *	Enable/disable offloading NPU.	option	-

Option	Description
enable	Enable NPU offloading.
disable	Disable NPU offloading.

send-cert-chain	Enable/disable sending certificate chain.	option	-

Option	Description
enable	Enable sending certificate chain.
disable	Disable sending certificate chain.

dhgrp	DH group.	option	-

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
	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	-
	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	-
	Option **Description** *enable* Enable IKEv2 EAP authentication. *disable* Disable IKEv2 EAP authentication.		
eap-identity	IKEv2 EAP peer identity type.	option	-
	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	-

Parameter	Description	Type	Size
	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	-
	Option / **Description** *disable* — Disable use of IKEv2 Postquantum Preshared Key (PPK). *allow* — Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK). *require* — 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	-
	Option / **Description** *custom* — Custom VPN configuration. *dialup-forticlient* — Dial Up - FortiClient Windows, Mac and Android. *dialup-ios* — Dial Up - iPhone / iPad Native IPsec Client. *dialup-android* — Dial Up - Android Native IPsec Client. *dialup-windows* — Dial Up - Windows Native IPsec Client. *dialup-cisco* — Dial Up - Cisco IPsec Client. *static-fortigate* — Site to Site - FortiGate. *dialup-fortigate* — Dial Up - FortiGate. *static-cisco* — Site to Site - Cisco. *dialup-cisco-fw* — Dialup Up - Cisco Firewall. *simplified-static-fortigate* — Site to Site - FortiGate (SD-WAN). *hub-fortigate-auto-discovery* — Hub role in a Hub-and-Spoke auto-discovery VPN. *spoke-fortigate-auto-discovery* — Spoke role in a Hub-and-Spoke auto-discovery VPN.		

Parameter	Description	Type	Size
xauthtype	XAuth type.	option	-

Option	Description
disable	Disable.
client	Enable as client.
pap	Enable as server PAP.
chap	Enable as server CHAP.
auto	Enable as server auto.

Parameter	Description	Type	Size
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-

Option	Description
disable	Disable IKE SA re-authentication.
enable	Enable IKE SA re-authentication.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable IKEv2 IDi group authentication.
disable	Disable IKEv2 IDi group authentication.

Parameter	Description	Type	Size
group-authentication-secret	Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by a leading 0x.)	password-3	Not Specified
authusrgrp	Authentication user group.	string	Maximum length: 35
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-

Option	Description
disable	Disable.
subnet	Enable addition of matching subnet selector.
host	Enable addition of host to host selector.

Parameter	Description	Type	Size
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-

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
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-

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	-

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	-

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	-

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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable use of pre-shared-secret authentication for auto-discovery tunnels. *disable* — Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.		
encapsulation	Enable/disable GRE/VXLAN encapsulation.	option	-
	Option / **Description** *none* — No additional encapsulation. *gre* — GRE encapsulation. *vxlan* — VXLAN encapsulation.		
encapsulation-address	Source for GRE/VXLAN tunnel address.	option	-
	Option / **Description** *ike* — Use IKE/IPsec gateway addresses. *ipv4* — Specify separate GRE/VXLAN tunnel address. *ipv6* — Specify separate GRE/VXLAN tunnel address.		
encap-local-gw4	Local IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified
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
encap-remote-gw6	Remote IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified
vni	VNI of VXLAN tunnel.	integer	Minimum value: 1 Maximum value: 16777215
nattraversal	Enable/disable NAT traversal.	option	-
	Option / **Description** *enable* — Enable IPsec NAT traversal. *disable* — Disable IPsec NAT traversal. *forced* — Force IPsec NAT traversal on.		

Parameter	Description	Type	Size
fragmentation-mtu	IKE fragmentation MTU .	integer	Minimum value: 500 Maximum value: 16000
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-

Option	Description
enable	Enable childless IKEv2 initiation (RFC 6023).
disable	Disable childless IKEv2 initiation (RFC 6023).

rekey	Enable/disable phase1 rekey.	option	-

Option	Description
enable	Enable phase1 rekey.
disable	Disable phase1 rekey.

digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-

Option	Description
enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).
disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).

signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-

Option	Description
sha1	SHA1.
sha2-256	SHA2-256.
sha2-384	SHA2-384.
sha2-512	SHA2-512.

rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-

Option	Description
pkcs1	RSASSA PKCS#1 v1.5.
pss	RSASSA Probabilistic Signature Scheme (PSS).

Parameter	Description	Type	Size
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-

Option	Description
disable	Disable peer ID uniqueness enforcement.
keep-new	Enforce peer ID uniqueness, keep new connection if collision found.
keep-old	Enforce peer ID uniqueness, keep old connection if collision found.

Parameter	Description	Type	Size
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-

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.

Parameter	Description	Type	Size
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-

Option	Description
enable	Enable Forward Error Correction for egress IPsec traffic.
disable	Disable Forward Error Correction for egress IPsec traffic.

Parameter	Description	Type	Size
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 1000
fec-base	Number of base Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100
fec-redundant	Number of redundant Forward Error Correction packets .	integer	Minimum value: 1 Maximum value: 100
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-

Parameter	Description	Type	Size
	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
network-overlay	Enable/disable network overlays.	option	-
	Option / **Description** *disable* / Disable network overlays. *enable* / Enable network overlays.		
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified

config ipv6-exclude-range

Parameter	Description	Type	Size
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 keylifekbs {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 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
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
proposal	Phase2 proposal.	option	-

Option	Description
null-md5	null-md5
null-sha1	null-sha1
null-sha256	null-sha256
null-sha384	null-sha384
null-sha512	null-sha512
des-null	des-null
des-md5	des-md5
des-sha1	des-sha1
des-sha256	des-sha256
des-sha384	des-sha384
des-sha512	des-sha512
3des-null	3des-null
3des-md5	3des-md5
3des-sha1	3des-sha1
3des-sha256	3des-sha256
3des-sha384	3des-sha384
3des-sha512	3des-sha512
aes128-null	aes128-null
aes128-md5	aes128-md5
aes128-sha1	aes128-sha1
aes128-sha256	aes128-sha256
aes128-sha384	aes128-sha384
aes128-sha512	aes128-sha512
aes128gcm	aes128gcm
aes192-null	aes192-null
aes192-md5	aes192-md5
aes192-sha1	aes192-sha1
aes192-sha256	aes192-sha256

Parameter	Description	Type	Size

Option	Description
aes192-sha384	aes192-sha384
aes192-sha512	aes192-sha512
aes256-null	aes256-null
aes256-md5	aes256-md5
aes256-sha1	aes256-sha1
aes256-sha256	aes256-sha256
aes256-sha384	aes256-sha384
aes256-sha512	aes256-sha512
aes256gcm	aes256gcm
chacha20poly1305	chacha20poly1305

pfs	Enable/disable PFS feature.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-

Option	Description
enable	Set IPv4 DF.
disable	Reset IPv4 DF.

dhgrp	Phase2 DH group.	option	-

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.

Parameter	Description	Type	Size
	Option **Description** *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	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
keepalive	Enable/disable keep alive.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
add-route	Enable/disable automatic route addition.	option	-
	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.		

Parameter	Description	Type	Size
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-

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
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-

Option	Description
phase1	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.
enable	Enable forwarding auto-discovery short-cut messages.
disable	Disable forwarding auto-discovery short-cut messages.

Parameter	Description	Type	Size
keylifeseconds	Phase2 key life in time in seconds .	integer	Minimum value: 120 Maximum value: 172800
keylifekbs	Phase2 key life in number of bytes of traffic .	integer	Minimum value: 5120 Maximum value: 4294967295
keylife-type	Keylife type.	option	-

Option	Description
seconds	Key life in seconds.
kbs	Key life in kilobytes.
both	Key life both.

Parameter	Description	Type	Size
single-source	Enable/disable single source IP restriction.	option	-

Option	Description
enable	Only single source IP will be accepted.
disable	Source IP range will be accepted.

Parameter	Description	Type	Size
route-overlap	Action for overlapping routes.	option	-

Option	Description
use-old	Use the old route and do not add the new route.
use-new	Delete the old route and add the new route.
allow	Allow overlapping routes.

Parameter	Description	Type	Size
encapsulation	ESP encapsulation mode.	option	-

Option	Description
tunnel-mode	Use tunnel mode encapsulation.
transport-mode	Use transport mode encapsulation.

Parameter	Description	Type	Size
l2tp	Enable/disable L2TP over IPsec.	option	-

Option	Description
enable	Enable L2TP over IPsec.
disable	Disable L2TP over IPsec.

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 255
protocol	Quick mode protocol selector .	integer	Minimum value: 0 Maximum value: 255
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	-

Option	Description
subnet	IPv4 subnet.
range	IPv4 range.
ip	IPv4 IP.
name	IPv4 firewall address or group name.
subnet6	IPv6 subnet.

Parameter	Description	Type	Size
	Option **Description** *range6* IPv6 range. *ip6* IPv6 IP. *name6* IPv6 firewall address or group name.		
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
src-port	Quick mode source port .	integer	Minimum value: 0 Maximum value: 65535
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	-
	Option **Description** *subnet* IPv4 subnet. *range* IPv4 range. *ip* IPv4 IP. *name* IPv4 firewall address or group name. *subnet6* IPv6 subnet. *range6* IPv6 range. *ip6* IPv6 IP. *name6* IPv6 firewall address or group name.		
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified

Parameter	Description	Type	Size
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
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
dst-port	Quick mode destination port .	integer	Minimum value: 0 Maximum value: 65535

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
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15
ip-version	IP version to use for VPN interface.	option	-

Parameter	Description	Type	Size
	Option / **Description** *4* — Use IPv4 addressing for gateways. *6* — Use IPv6 addressing for gateways.		
addr-type	IP version to use for IP packets.	option	-
	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
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
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	-
	Option / **Description** *null* — null *md5* — md5 *sha1* — sha1 *sha256* — sha256 *sha384* — sha384 *sha512* — sha512		
enc-alg	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-
	Option / **Description** *null* — null *des* — des *3des* — 3des *aes128* — aes128 *aes192* — aes192		

Parameter	Description	Type	Size
	Option **Description** *aes256* aes256		
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	-
	Option **Description** *enable* Enable NPU offloading. *disable* 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
usergroupname	User group name for FortiClient users.	string	Maximum length: 35

Parameter	Description	Type	Size
phase2name	Phase 2 tunnel name that you defined in the FortiClient dialup configuration.	string	Maximum length: 35
status	Enable/disable this FortiClient configuration.	option	-

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
status	Enable/disable FortiGate as a PPTP gateway.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
ip-mode	IP assignment mode for PPTP client.	option	-
	Option / **Description** *range* — PPTP client IP from manual config (range from sip to eip). *usrgrp* — PPTP client IP from user-group defined server.		
eip	End IP.	ipv4-address	Not Specified
sip	Start IP.	ipv4-address	Not Specified
local-ip	Local IP to be used for peer's remote IP.	ipv4-address	Not Specified
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 compress [enable|disable]
end
```

config vpn l2tp

Parameter	Description	Type	Size
status	Enable/disable FortiGate as a L2TP gateway.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
eip	End IP.	ipv4-address	Not Specified
sip	Start IP.	ipv4-address	Not Specified
usrgrp	User group.	string	Maximum length: 35
enforce-ipsec	Enable/disable IPsec enforcement.	option	-

Option	Description
enable	Enable enforce-ipsec
disable	Disable enforce-ipsec

Parameter	Description	Type	Size
compress	Enable/disable data compression.	option	-

Option	Description
enable	Enable compress
disable	Disable compress

config vpn ocvpn

Configure Overlay Controller VPN settings.

```
config vpn ocvpn
   Description: Configure Overlay Controller VPN settings.
   set status [enable|disable]
   set role [spoke|primary-hub|...]
   set poll-interval {integer}
   set auto-discovery [enable|disable]
```

```
   set eap [enable|disable]
   set eap-users {string}
   set nat [enable|disable]
   config overlays
      Description: Network overlays to register with Overlay Controller VPN service.
      edit <id>
         set name {string}
         set assign-ip [enable|disable]
         set ipv4-start-ip {ipv4-address}
         set ipv4-end-ip {ipv4-address}
         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
end
```

config vpn ocvpn

Parameter	Description	Type	Size
status	Enable/disable Overlay Controller cloud assisted VPN.	option	-

Option	Description
enable	Enable Overlay Controller VPN.
disable	Disable Overlay Controller VPN.

Parameter	Description	Type	Size
role	Set device role.	option	-

Option	Description
spoke	Register device as static spoke.
primary-hub	Register device as primary hub.
secondary-hub	Register device as secondary hub.

Parameter	Description	Type	Size
poll-interval	Overlay Controller VPN polling interval.	integer	Minimum value: 30 Maximum value: 120
auto-discovery	Enable/disable auto-discovery shortcuts.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable ADVPN auto-discovery shortcuts. *disable* — Disable ADVPN auto-discovery shortcuts.		
eap	Enable/disable EAP client authentication.	option	-
	Option / **Description** *enable* — Enable EAP client authentication. *disable* — Disable EAP client authentication.		
eap-users	EAP authentication user group.	string	Maximum length: 35
nat	Enable/disable inter-overlay source NAT.	option	-
	Option / **Description** *enable* — Enable inter-overlay source NAT. *disable* — Disable inter-overlay source NAT.		

config overlays

Parameter	Description	Type	Size
name	Overlay name.	string	Maximum length: 63
assign-ip	Enable/disable client address assignment.	option	-
	Option / **Description** *enable* — Enable client IPv4 address assignment. *disable* — Disable client IPv4 address assignment.		
ipv4-start-ip	Start of client IPv4 range.	ipv4-address	Not Specified
ipv4-end-ip	End of client IPv4 range.	ipv4-address	Not Specified

config subnets

Parameter	Description	Type	Size
type	Subnet type.	option	-

Parameter	Description	Type	Size
	Option / **Description** *subnet* — Configure participating subnet IP and mask. *interface* — Configure participating LAN interface.		
subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified
interface	LAN interface.	string	Maximum length: 15

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
<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 signature on page 1277
- config waf sub-class on page 1276
- config waf profile on page 1277
- config waf main-class on page 1276

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
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
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
desc	Signature description.	string	Maximum length: 511

config waf profile

Web application firewall configuration.

```
config waf profile
   Description: Web application firewall configuration.
   edit <name>
      set external [disable|enable]
      set extended-log [enable|disable]
      config signature
         Description: WAF signatures.
         config main-class
            Description: Main signature class.
            edit <id>
               set status [enable|disable]
               set action [allow|block|...]
               set log [enable|disable]
               set severity [high|medium|...]
            next
         end
         set disabled-sub-class <id1>, <id2>, ...
         set disabled-signature <id1>, <id2>, ...
         set credit-card-detection-threshold {integer}
         config custom-signature
            Description: Custom signature.
            edit <name>
               set status [enable|disable]
               set action [allow|block|...]
               set log [enable|disable]
               set severity [high|medium|...]
               set direction [request|response]
               set case-sensitivity [disable|enable]
               set pattern {string}
               set target {option1}, {option2}, ...
            next
         end
```

```
    end
    config constraint
       Description: WAF HTTP protocol restrictions.
       config header-length
          Description: HTTP header length in request.
          set status [enable|disable]
          set length {integer}
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
       config content-length
          Description: HTTP content length in request.
          set status [enable|disable]
          set length {integer}
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
       config param-length
          Description: Maximum length of parameter in URL, HTTP POST request or HTTP body.
          set status [enable|disable]
          set length {integer}
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
       config line-length
          Description: HTTP line length in request.
          set status [enable|disable]
          set length {integer}
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
       config url-param-length
          Description: Maximum length of parameter in URL.
          set status [enable|disable]
          set length {integer}
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
       config version
          Description: Enable/disable HTTP version check.
          set status [enable|disable]
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
       config method
          Description: Enable/disable HTTP method check.
          set status [enable|disable]
          set action [allow|block]
          set log [enable|disable]
          set severity [high|medium|...]
       end
```

```
config hostname
   Description: Enable/disable hostname check.
   set status [enable|disable]
   set action [allow|block]
   set log [enable|disable]
   set severity [high|medium|...]
end
config malformed
   Description: Enable/disable malformed HTTP request check.
   set status [enable|disable]
   set action [allow|block]
   set log [enable|disable]
   set severity [high|medium|...]
end
config max-cookie
   Description: Maximum number of cookies in HTTP request.
   set status [enable|disable]
   set max-cookie {integer}
   set action [allow|block]
   set log [enable|disable]
   set severity [high|medium|...]
end
config max-header-line
   Description: Maximum number of HTTP header line.
   set status [enable|disable]
   set max-header-line {integer}
   set action [allow|block]
   set log [enable|disable]
   set severity [high|medium|...]
end
config max-url-param
   Description: Maximum number of parameters in URL.
   set status [enable|disable]
   set max-url-param {integer}
   set action [allow|block]
   set log [enable|disable]
   set severity [high|medium|...]
end
config max-range-segment
   Description: Maximum number of range segments in HTTP range line.
   set status [enable|disable]
   set max-range-segment {integer}
   set action [allow|block]
   set log [enable|disable]
   set severity [high|medium|...]
end
config exception
   Description: HTTP constraint exception.
   edit <id>
      set pattern {string}
      set regex [enable|disable]
      set address {string}
      set header-length [enable|disable]
      set content-length [enable|disable]
      set param-length [enable|disable]
      set line-length [enable|disable]
      set url-param-length [enable|disable]
```

```
            set version [enable|disable]
            set method [enable|disable]
            set hostname [enable|disable]
            set malformed [enable|disable]
            set max-cookie [enable|disable]
            set max-header-line [enable|disable]
            set max-url-param [enable|disable]
            set max-range-segment [enable|disable]
         next
      end
   end
   config method
      Description: Method restriction.
      set status [enable|disable]
      set log [enable|disable]
      set severity [high|medium|...]
      set default-allowed-methods {option1}, {option2}, ...
      config method-policy
         Description: HTTP method policy.
         edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}
            set allowed-methods {option1}, {option2}, ...
         next
      end
   end
   config address-list
      Description: Black address list and white address list.
      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
external	Disable/Enable external HTTP Inspection.	option	-

Option	Description
disable	Disable external inspection.
enable	Enable external inspection.

Parameter	Description	Type	Size
extended-log	Enable/disable extended logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 1023

config signature

Parameter	Description	Type	Size
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

config main-class

Parameter	Description	Type	Size
status	Status.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block. *erase* Erase credit card numbers.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config custom-signature

Parameter	Description	Type	Size
status	Status.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		

Parameter	Description	Type	Size
	Option **Description** *erase* Erase credit card numbers.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		
direction	Traffic direction.	option	-
	Option **Description** *request* Match HTTP request. *response* Match HTTP response.		
case-sensitivity	Case sensitivity in pattern.	option	-
	Option **Description** *disable* Case insensitive in pattern. *enable* Case sensitive in pattern.		
pattern	Match pattern.	string	Maximum length: 511
target	Match HTTP target.	option	-
	Option **Description** *arg* HTTP arguments. *arg-name* Names of HTTP arguments. *req-body* HTTP request body. *req-cookie* HTTP request cookies. *req-cookie-name* HTTP request cookie names.		

Parameter	Description	Type	Size
	Option **Description** *req-filename* HTTP request file name. *req-header* HTTP request headers. *req-header-name* HTTP request header names. *req-raw-uri* Raw URI of HTTP request. *req-uri* URI of HTTP request. *resp-body* HTTP response body. *resp-hdr* HTTP response headers. *resp-status* HTTP response status.		

config header-length

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-

Parameter	Description	Type	Size
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config content-length

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config param-length

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
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
action	Action.	option	-

Option	Description
allow	Allow.
block	Block.

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

config line-length

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-

Option	Description
allow	Allow.
block	Block.

log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

config url-param-length

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-

Parameter	Description	Type	Size
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config version

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-

Parameter	Description	Type	Size
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config method

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config method

Parameter	Description	Type	Size
status	Status.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity *medium* medium severity *low* low severity		
default-allowed-methods	Methods.	option	-
	Option **Description** *get* HTTP GET method. *post* HTTP POST method. *put* HTTP PUT method. *head* HTTP HEAD method. *connect* HTTP CONNECT method. *trace* HTTP TRACE method. *options* HTTP OPTIONS method. *delete* HTTP DELETE method. *others* Other HTTP methods.		

config hostname

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config malformed

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
severity	Severity.	option	-
	Option / **Description** *high* / High severity. *medium* / Medium severity. *low* / Low severity.		

config max-cookie

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-
	Option / **Description** *allow* / Allow. *block* / Block.		
log	Enable/disable logging.	option	-
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.		
severity	Severity.	option	-

Parameter	Description	Type	Size
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config max-header-line

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-
	Option **Description** *allow* Allow. *block* Block.		
log	Enable/disable logging.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
severity	Severity.	option	-
	Option **Description** *high* High severity. *medium* Medium severity. *low* Low severity.		

config max-url-param

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-

Option	Description
allow	Allow.
block	Block.

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

config max-range-segment

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
action	Action.	option	-

Option	Description
allow	Allow.
block	Block.

log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

config exception

Parameter	Description	Type	Size
pattern	URL pattern.	string	Maximum length: 511
regex	Enable/disable regular expression based pattern match.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

address	Host address.	string	Maximum length: 79
header-length	HTTP header length in request.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
content-length	HTTP content length in request.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
line-length	HTTP line length in request.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
url-param-length	Maximum length of parameter in URL.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
version	Enable/disable HTTP version check.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
method	Enable/disable HTTP method check.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
hostname	Enable/disable hostname check.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
malformed	Enable/disable malformed HTTP request check.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
max-cookie	Maximum number of cookies in HTTP request.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
max-header-line	Maximum number of HTTP header line.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
max-url-param	Maximum number of parameters in URL.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
max-range-segment	Maximum number of range segments in HTTP range line.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

config method

Parameter	Description	Type	Size
status	Enable/disable the constraint.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
action	Action.	option	-

Option	Description
allow	Allow.
block	Block.

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

config method

Parameter	Description	Type	Size
status	Status.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		
severity	Severity.	option	-
	Option / **Description** *high* — High severity *medium* — medium severity *low* — low severity		
default-allowed-methods	Methods.	option	-
	Option / **Description** *get* — HTTP GET method. *post* — HTTP POST method. *put* — HTTP PUT method. *head* — HTTP HEAD method. *connect* — HTTP CONNECT method. *trace* — HTTP TRACE method. *options* — HTTP OPTIONS method. *delete* — HTTP DELETE method. *others* — Other HTTP methods.		

config method-policy

Parameter	Description	Type	Size
pattern	URL pattern.	string	Maximum length: 511
regex	Enable/disable regular expression based pattern match.	option	-
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.		

Parameter	Description	Type	Size
address	Host address.	string	Maximum length: 79
allowed-methods	Allowed Methods.	option	-

Option	Description
get	HTTP GET method.
post	HTTP POST method.
put	HTTP PUT method.
head	HTTP HEAD method.
connect	HTTP CONNECT method.
trace	HTTP TRACE method.
options	HTTP OPTIONS method.
delete	HTTP DELETE method.
others	Other HTTP methods.

config address-list

Parameter	Description	Type	Size
status	Status.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

blocked-log	Enable/disable logging on blocked addresses.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

Parameter	Description	Type	Size
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79

config url-access

Parameter	Description	Type	Size
address	Host address.	string	Maximum length: 79
action	Action.	option	-

Option	Description
bypass	Allow the HTTP request, also bypass further WAF scanning.
permit	Allow the HTTP request, and continue further WAF scanning.
block	Block HTTP request.

log	Enable/disable logging.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

severity	Severity.	option	-

Option	Description
high	High severity.
medium	Medium severity.
low	Low severity.

config access-pattern

Parameter	Description	Type	Size
srcaddr	Source address.	string	Maximum length: 79
pattern	URL pattern.	string	Maximum length: 511

Parameter	Description	Type	Size
regex	Enable/disable regular expression based pattern match.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
negate	Enable/disable match negation.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

web-proxy

This section includes syntax for the following commands:

- config web-proxy url-match on page 1318
- config web-proxy wisp on page 1318
- config web-proxy global on page 1307
- config web-proxy forward-server-group on page 1315
- config web-proxy profile on page 1303
- config web-proxy debug-url on page 1317
- config web-proxy forward-server on page 1314
- config web-proxy explicit on page 1309

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-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
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-

Option	Description
pass	Forward the same HTTP header.
add	Add the HTTP header.
remove	Remove the HTTP header.

Parameter	Description	Type	Size
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-

Option	Description
pass	Forward the same HTTP header.
add	Add the HTTP header.
remove	Remove the HTTP header.

Parameter	Description	Type	Size
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-

Option	Description
pass	Forward the same HTTP header.
add	Add the HTTP header.
remove	Remove the HTTP header.

Parameter	Description	Type	Size
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	-

Option	Description
pass	Forward the same HTTP header.
add	Add the HTTP header.
remove	Remove the HTTP header.

Parameter	Description	Type	Size
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	-

Parameter	Description	Type	Size
	Option **Description** *pass* Forward the same HTTP header. *add* Add the HTTP header. *remove* 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	-
	Option **Description** *pass* Forward the same HTTP header. *add* Add the HTTP header. *remove* 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	-
	Option **Description** *pass* Forward the same HTTP header. *add* Add the HTTP header. *remove* Remove the HTTP header.		
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-
	Option **Description** *enable* Enable stripping of unsupported encoding from the request header. *disable* Disable stripping of unsupported encoding from the request header.		
log-header-change	Enable/disable logging HTTP header changes.	option	-
	Option **Description** *enable* Enable Enable/disable logging HTTP header changes. *disable* Disable Enable/disable logging HTTP header changes.		

config headers

Parameter	Description	Type	Size
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	-

Option	Description
add-to-request	Add the HTTP header to request.
add-to-response	Add the HTTP header to response.
remove-from-request	Remove the HTTP header from request.
remove-from-response	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	-

Option	Description
disable	Disable use of base64 encoding of HTTP content.
enable	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	-

Option	Description
append	Append content to existing HTTP header or create new header if HTTP header is not found.
new-on-not-found	Create new header only if existing HTTP header is not found.
new	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	-

Parameter	Description	Type	Size

Option	Description
https	Perform add-option action on HTTPS.
http	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 tunnel-non-http [enable|disable]
   set unknown-http-version [reject|tunnel|...]
   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>, ...
end
```

config web-proxy global

Parameter	Description	Type	Size
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
proxy-fqdn	Fully Qualified Domain Name to connect to the explicit web proxy.	string	Maximum length: 255
max-request-length	Maximum length of HTTP request line .	integer	Minimum value: 2 Maximum value: 64
max-message-length	Maximum length of HTTP message, not including body .	integer	Minimum value: 16 Maximum value: 256
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	-

Option	Description
enable	Enable strict web checking.
disable	Disable strict web checking.

forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-

Option	Description
enable	Enable forwarding proxy authentication headers.
disable	Disable forwarding proxy authentication headers.

tunnel-non-http	Enable/disable allowing non-HTTP traffic. Allowed non-HTTP traffic is tunneled.	option	-

Option	Description
enable	Allow non-HTTP traffic.
disable	Block non-HTTP traffic.

unknown-http-version	Action to take when an unknown version of HTTP is encountered: reject, allow (tunnel), or proceed with best-effort.	option	-

Option	Description
reject	Rejects requests with unknown HTTP version.
tunnel	Tunnels requests with unknown HTTP version.
best-effort	Allow unknown HTTP requests and process them using best efforts.

Parameter	Description	Type	Size
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
max-waf-body-cache-length	Maximum length of HTTP messages processed by Web Application Firewall .	integer	Minimum value: 10 Maximum value: 1024
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	-

Option	Description
enable	Enable learning the client's IP address from headers.
disable	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
true-client-ip	Learn the client IP address from the True-Client-IP header.
x-real-ip	Learn the client IP address from the X-Real-IP header.
x-forwarded-for	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

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
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-

Option	Description
enable	Enable the explicit web proxy.
disable	Disable the explicit web proxy.

ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable FTP-over-HTTP sessions. *disable* Disable FTP-over-HTTP sessions.		
socks	Enable/disable the SOCKS proxy.	option	-
	Option **Description** *enable* Enable the SOCKS proxy. *disable* 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
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	-
	Option **Description** *enable* Enable allowing an IPv6 web proxy destination. *disable* Disable allowing an IPv6 web proxy destination.		
incoming-ip6	Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified
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
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-

Option	Description
enable	Enable strict guest user checking.
disable	Disable strict guest user checking.

Parameter	Description	Type	Size
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server .	option	-

Option	Description
ipv4	Prefer the IPv4 DNS server.
ipv6	Prefer the IPv6 DNS server.

Parameter	Description	Type	Size
unknown-http-version	Either reject unknown HTTP traffic as malformed or handle unknown HTTP traffic as best as the proxy server can.	option	-

Option	Description
reject	Reject requests with an unknown HTTP version.
best-effort	Accept requests with an unknown HTTP version and use best efforts to handle the session.

Parameter	Description	Type	Size
realm	Authentication realm used to identify the explicit web proxy (maximum of 63 characters).	string	Maximum length: 63
sec-default-action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.	option	-

Option	Description
accept	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.
deny	Deny requests unless there is a matching explicit web proxy policy.

Parameter	Description	Type	Size
https-replacement-message	Enable/disable sending the client a replacement message for HTTPS requests.	option	-

Option	Description
enable	Display a replacement message for HTTPS requests.
disable	Do not display a replacement message for HTTPS requests.

Parameter	Description	Type	Size
message-upon-server-error	Enable/disable displaying a replacement message when a server error is detected.	option	-

Option	Description
enable	Display a replacement message when a server error is detected.
disable	Do not display a replacement message when a server error is detected.

Parameter	Description	Type	Size
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-

Option	Description
enable	Enable Proxy Auto-Configuration (PAC).
disable	Disable Proxy Auto-Configuration (PAC).

Parameter	Description	Type	Size
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
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	-

Option	Description
high	High encrption. Allow only AES and ChaCha.
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.

Parameter	Description	Type	Size
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-

Option	Description
enable	Enable logging timed-out authentication requests.
disable	Disable logging timed-out authentication requests.

config pac-policy

Parameter	Description	Type	Size
status	Enable/disable policy.	option	-
	Option / **Description** *enable* — Enable policy. *disable* — 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
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 comment {string}
   next
end
```

config web-proxy forward-server

Parameter	Description	Type	Size
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-

Option	Description
ip	Use an IP address for the forwarding proxy server.
fqdn	Use the FQDN for the forwarding proxy server.

Parameter	Description	Type	Size
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255
port	Port number that the forwarding server expects to receive HTTP sessions on .	integer	Minimum value: 1 Maximum value: 65535
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	-

Option	Description
disable	Disable health checking.
enable	Enable health checking.

Parameter	Description	Type	Size
monitor	URL for forward server health check monitoring .	string	Maximum length: 255
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	-

Option	Description
block	Block sessions until the server is back up.
pass	Pass sessions to their destination bypassing the forward server.

Parameter	Description	Type	Size
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
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	-

Option	Description
enable	Enable affinity.
disable	Disable affinity.

Parameter	Description	Type	Size
ldb-method	Load balance method: weighted or least-session.	option	-

Option	Description
weighted	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.
least-session	Send new sessions to the server with lowest session count.
active-passive	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.

Parameter	Description	Type	Size
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	-

Option	Description
block	Block sessions until at least one server in the group is back up.

Parameter	Description	Type	Size

Option	Description
pass	Pass sessions to their destination bypassing servers in the forward server group.

config server-list

Parameter	Description	Type	Size
weight	Optionally assign a weight of the forwarding server for weighted load balancing	integer	Minimum value: 1 Maximum value: 100

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
url-pattern	URL exemption pattern.	string	Maximum length: 511
status	Enable/disable this URL exemption.	option	-

Option	Description
enable	Enable this URL exemption.
disable	Disable this URL exemption.

exact	Enable/disable matching the exact path.	option	-

Option	Description
enable	Enable matching the exact path.
disable	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
comment	Comment.	var-string	Maximum length: 255
outgoing-ip	WISP outgoing IP address.	ipv4-address-any	Not Specified
server-ip	WISP server IP address.	ipv4-address-any	Not Specified
server-port	WISP server port .	integer	Minimum value: 1 Maximum value: 65535
max-connections	Maximum number of web proxy WISP connections .	integer	Minimum value: 4 Maximum value: 4096
timeout	Period of time before WISP requests time out .	integer	Minimum value: 1 Maximum value: 15

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
status	Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding and caching.	option	-

Option	Description
enable	Enable exempting the matching URLs.
disable	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	-

Option	Description
enable	Enable exempting this URL pattern from caching.
disable	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 override-usr on page 1348
- config webfilter categories on page 1345
- config webfilter urlfilter on page 1323
- config webfilter profile on page 1327
- config webfilter fortiguard on page 1343
- config webfilter ips-urlfilter-setting on page 1326
- config webfilter search-engine on page 1347
- config webfilter override on page 1345
- config webfilter ftgd-local-cat on page 1320
- config webfilter ips-urlfilter-setting6 on page 1326
- config webfilter ftgd-local-rating on page 1346
- config webfilter ips-urlfilter-cache-setting on page 1327
- config webfilter ftgd-statistics on page 1348
- config webfilter status on page 1348
- config webfilter content-header on page 1322
- config webfilter content on page 1321

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
status	Enable/disable the local category.	option	-

Option	Description
enable	Enable the local category.
disable	Disable the local category.

Parameter	Description	Type	Size
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191

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

config entries

Parameter	Description	Type	Size
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-

Option	Description
wildcard	Wildcard pattern.
regexp	Perl regular expression.

Parameter	Description	Type	Size
status	Enable/disable banned word.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
lang	Language of banned word.	option	-

Option	Description
western	Western.
simch	Simplified Chinese.
trach	Traditional Chinese.
japanese	Japanese.
korean	Korean.
french	French.
thai	Thai.
spanish	Spanish.
cyrillic	Cyrillic.

Parameter	Description	Type	Size
score	Score, to be applied every time the word appears on a web page .	integer	Minimum value: 0 Maximum value: 4294967295
action	Block or exempt word when a match is found.	option	-

Option	Description
block	Block matches.
exempt	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
name	Name of table.	string	Maximum length: 63
comment	Optional comments.	var-string	Maximum length: 255

config entries

Parameter	Description	Type	Size
action	Action to take for this content type.	option	-

Option	Description
block	Block content type.
allow	Allow content type.
exempt	Exempt content type.

category	Categories that this content type applies to.	user	Not Specified

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 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
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	-

Option	Description
enable	Enable DNS resolver for one-arm IPS URL filter operation.
disable	Disable DNS resolver for one-arm IPS URL filter operation.

Parameter	Description	Type	Size
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-

Option	Description
enable	Enable blocking URLs when the hostname appears as an IP address.
disable	Disable blocking URLs when the hostname appears as an IP address.

config entries

Parameter	Description	Type	Size
url	URL to be filtered.	string	Maximum length: 511
type	Filter type (simple, regex, or wildcard).	option	-

Option	Description
simple	Simple URL string.
regex	Regular expression URL string.
wildcard	Wildcard URL string.

Parameter	Description	Type	Size
action	Action to take for URL filter matches.	option	-

Parameter	Description	Type	Size
	Option / **Description** *exempt* — Exempt matches. *block* — Block matches. *allow* — Allow matches (no log). *monitor* — Allow matches (with log).		
status	Enable/disable this URL filter.	option	-
	Option / **Description** *enable* — Enable this URL filter. *disable* — 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	-
	Option / **Description** *av* — AntiVirus scanning. *web-content* — Web filter content matching. *activex-java-cookie* — ActiveX, Java, and cookie filtering. *dlp* — DLP scanning. *fortiguard* — FortiGuard web filtering. *range-block* — Range block feature. *pass* — Pass single connection from all. *all* — 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	-
	Option / **Description** *ipv4* — Resolve IPv4 address from DNS server.		

Parameter	Description	Type	Size

Option	Description
ipv6	Resolve IPv6 address from DNS server.
both	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
device	Interface for this route.	string	Maximum length: 35
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255
gateway	Gateway IP address for this route.	ipv4-address	Not Specified
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
device	Interface for this route.	string	Maximum length: 35
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255
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
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
extended-ttl	Extend time to live beyond reported by DNS. 0 means use DNS server's TTL	integer	Minimum value: 0 Maximum value: 2147483

config webfilter profile

Configure Web filter profiles.

```
config webfilter profile
   Description: Configure Web filter profiles.
   edit <name>
      set comment {var-string}
      set replacemsg-group {string}
```

```
set options {option1}, {option2}, ...
config file-filter
   Description: File filter.
   set status [enable|disable]
   set log [enable|disable]
   set scan-archive-contents [enable|disable]
   config entries
      Description: File filter entries.
      edit <filter>
         set comment {var-string}
         set protocol {option1}, {option2}, ...
         set action [log|block]
         set direction [incoming|outgoing|...]
         set password-protected [yes|any]
         set file-type <name1>, <name2>, ...
      next
   end
end
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 blacklist [enable|disable]
   set whitelist {option1}, {option2}, ...
   set safe-search {option1}, {option2}, ...
   set youtube-restrict [none|strict|...]
   set log-search [enable|disable]
   set keyword-match <pattern1>, <pattern2>, ...
end
set youtube-channel-status [disable|blacklist|...]
config youtube-channel-filter
   Description: YouTube channel filter.
   edit <id>
      set channel-id {string}
      set comment {var-string}
   next
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-image-urls [disable|enable]
        set rate-javascript-urls [disable|enable]
        set rate-css-urls [disable|enable]
        set rate-crl-urls [disable|enable]
     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]
  next
end
```

config webfilter profile

Parameter	Description	Type	Size
comment	Optional comments.	var-string	Maximum length: 255
replacemsg-group	Replacement message group.	string	Maximum length: 35
options	Options.	option	-

Option	Description
activexfilter	ActiveX filter.
cookiefilter	Cookie filter.
javafilter	Java applet filter.
block-invalid-url	Block sessions contained an invalid domain name.
jscript	Javascript block.
js	JS block.
vbs	VB script block.
unknown	Unknown script block.
intrinsic	Intrinsic script block.
wf-referer	Referring block.
wf-cookie	Cookie block.

https-replacemsg	Enable replacement messages for HTTPS.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

ovrd-perm	Permitted override types.	option	-

Option	Description
bannedword-override	Banned word override.
urlfilter-override	URL filter override.
fortiguard-wf-override	FortiGuard Web Filter override.

Parameter	Description	Type	Size
	Option **Description** *contenttype-check-override* Content-type header override.		
post-action	Action taken for HTTP POST traffic.	option	-
	Option **Description** *normal* Normal, POST requests are allowed. *block* POST requests are blocked.		
youtube-channel-status	YouTube channel filter status.	option	-
	Option **Description** *disable* Disable YouTube channel filter. *blacklist* Block matches. *whitelist* Allow matches.		
wisp	Enable/disable web proxy WISP.	option	-
	Option **Description** *enable* Enable web proxy WISP. *disable* Disable web proxy WISP.		
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79
wisp-algorithm	WISP server selection algorithm.	option	-
	Option **Description** *primary-secondary* Select the first healthy server in order. *round-robin* Select the next healthy server. *auto-learning* Select the lightest loading healthy server.		
log-all-url	Enable/disable logging all URLs visited.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		

Parameter	Description	Type	Size
web-content-log	Enable/disable logging logging blocked web content.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
web-filter-activex-log	Enable/disable logging ActiveX.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
web-filter-applet-log	Enable/disable logging Java applets.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
web-filter-jscript-log	Enable/disable logging JScripts.	option	-

Option	Description
enable	Enable setting.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable setting.		
web-filter-js-log	Enable/disable logging Java scripts.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
web-filter-referer-log	Enable/disable logging referrers.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
web-url-log	Enable/disable logging URL filtering.	option	-

Parameter	Description	Type	Size
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
web-ftgd-err-log	Enable/disable logging rating errors.	option	-
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
extended-log	Enable/disable extended logging for web filtering.	option	-
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-
	Option: *enable* — Enable setting. Option: *disable* — Disable setting.		

config file-filter

Parameter	Description	Type	Size
status	Enable/disable file filter.	option	-

Option	Description
enable	Enable file filter.
disable	Disable file filter.

Parameter	Description	Type	Size
log	Enable/disable file filter logging.	option	-

Option	Description
enable	Enable file filter logging.
disable	Disable file filter logging.

Parameter	Description	Type	Size
scan-archive-contents	Enable/disable file filter archive contents scan.	option	-

Option	Description
enable	Enable file filter archive contents scan.
disable	Disable file filter archive contents scan.

config entries

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
protocol	Protocols to apply with.	option	-

Option	Description
http	Enable/disable HTTP.
ftp	Enable/disable FTP.

Parameter	Description	Type	Size
action	Action taken for matched file.	option	-

Option	Description
log	Allow the content and write a log message.
block	Block the content and write a log message.

Parameter	Description	Type	Size
direction	Match files transmitted in the session's originating or reply direction.	option	-

Parameter	Description	Type	Size
	Option **Description** *incoming* Match files transmitted in the session's originating direction. *outgoing* Match files transmitted in the session's reply direction. *any* Match files transmitted in the session's originating and reply direction.		
password-protected	Match password-protected files.	option	-
	Option **Description** *yes* Match only password-protected files. *any* Match any file.		
file-type <name>	Select file type. File type name.	string	Maximum length: 39

config override

Parameter	Description	Type	Size
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-
	Option **Description** *allow* Allow browser-based (cookie) override. *deny* Deny browser-based (cookie) override.		
ovrd-scope	Override scope.	option	-
	Option **Description** *user* Override for the user. *user-group* Override for the user's group. *ip* Override for the initiating IP. *browser* Create browser-based (cookie) override. *ask* Prompt for scope when initiating an override.		
profile-type	Override profile type.	option	-
	Option **Description** *list* Profile chosen from list. *radius* Profile determined by RADIUS server.		

Parameter	Description	Type	Size
ovrd-dur-mode	Override duration mode.	option	-

Option	Description
constant	Constant mode.
ask	Prompt for duration when initiating an override.

Parameter	Description	Type	Size
ovrd-dur	Override duration.	user	Not Specified
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
Class	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.

Parameter	Description	Type	Size
	Option / **Description** *Login-LAT-Service* / Use this attribute. *Login-LAT-Node* / Use this attribute. *Login-LAT-Group* / Use this attribute. *Framed-AppleTalk-Zone* / Use this attribute. *Acct-Session-Id* / Use this attribute. *Acct-Multi-Session-Id* / Use this attribute.		
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
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
blacklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blacklist.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
whitelist	FortiGuard whitelist settings.	option	-

Option	Description
exempt-av	Exempt antivirus.
exempt-webcontent	Exempt web content.
exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.
exempt-dlp	Exempt DLP.
exempt-rangeblock	Exempt RangeBlock.
extended-log-others	Support extended log.

Parameter	Description	Type	Size
safe-search	Safe search type.	option	-

Option	Description
url	Insert safe search string into URL.
header	Insert safe search header.

Parameter	Description	Type	Size
youtube-restrict	YouTube EDU filter level.	option	-

Option	Description
none	Full access for YouTube.
strict	Strict access for YouTube.
moderate	Moderate access for YouTube.

Parameter	Description	Type	Size
log-search	Enable/disable logging all search phrases.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79

config youtube-channel-filter

Parameter	Description	Type	Size
channel-id	YouTube channel ID to be filtered.	string	Maximum length: 255
comment	Comment.	var-string	Maximum length: 255

config ftgd-wf

Parameter	Description	Type	Size
options	Options for FortiGuard Web Filter.	option	-

Option	Description
error-allow	Allow web pages with a rating error to pass through.
rate-server-ip	Rate the server IP in addition to the domain name.
connect-request-bypass	Bypass connection which has CONNECT request.
ftgd-disable	Disable FortiGuard scanning.

exempt-quota	Do not stop quota for these categories.	user	Not Specified
ovrd	Allow web filter profile overrides.	user	Not Specified
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400
rate-image-urls	Enable/disable rating images by URL.	option	-

Option	Description
disable	Disable rating images by URL (blocked images are replaced with blanks).
enable	Enable rating images by URL (blocked images are replaced with blanks).

rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable rating JavaScript by URL. *enable* Enable rating JavaScript by URL.		
rate-css-urls	Enable/disable rating CSS by URL.	option	-
	Option **Description** *disable* Disable rating CSS by URL. *enable* Enable rating CSS by URL.		
rate-crl-urls	Enable/disable rating CRL by URL.	option	-
	Option **Description** *disable* Disable rating CRL by URL. *enable* Enable rating CRL by URL.		

config filters

Parameter	Description	Type	Size
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255
action	Action to take for matches.	option	-
	Option **Description** *block* Block access. *authenticate* Authenticate user before allowing access. *monitor* Allow access while logging the action. *warning* Allow access after warning the user.		
warn-duration	Duration of warnings.	user	Not Specified
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79
log	Enable/disable logging.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Enable setting. *disable* Disable setting.		
override-replacemsg	Override replacement message.	string	Maximum length: 28
warning-prompt	Warning prompts in each category or each domain.	option	-
	Option **Description** *per-domain* Per-domain warnings. *per-category* Per-category warnings.		
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-
	Option **Description** *session* After session ends. *timeout* After timeout occurs.		

config quota

Parameter	Description	Type	Size
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified
type	Quota type.	option	-
	Option **Description** *time* Use a time-based quota. *traffic* Use a traffic-based quota.		
unit	Traffic quota unit of measurement.	option	-
	Option **Description** *B* Quota in bytes. *KB* Quota in kilobytes. *MB* Quota in megabytes. *GB* Quota in gigabytes.		

Parameter	Description	Type	Size
value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295
duration	Duration of quota.	user	Not Specified
override-replacemsg	Override replacement message.	string	Maximum length: 28

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
cache-mode	Cache entry expiration mode.	option	-

Option	Description
ttl	Expire cache items by time-to-live.
db-ver	Expire cache items when the server DB version changes.

Parameter	Description	Type	Size
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
cache-mem-percent	Maximum percentage of available memory allocated to caching .	integer	Minimum value: 1 Maximum value: 15
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication	integer	Minimum value: 0 Maximum value: 65535
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535
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
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server .	integer	Minimum value: 576 Maximum value: 10000

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
status	Enable/disable override rule.	option	-

Option	Description
enable	Enable override rule.
disable	Disable override rule.

Parameter	Description	Type	Size
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-

Parameter	Description	Type	Size
	Option / **Description** *user* — Override the specified user. *user-group* — Override the specified user group. *ip* — Override the specified IP address. *ip6* — Override the specified IPv6 address.		
ip	IPv4 address which the override applies.	ipv4-address	Not Specified
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
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 rating {user}
   next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size
status	Enable/disable local rating.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable local rating. *disable* / Disable local rating.		
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
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	-
	Option / **Description** *disable* / Site does not support safe search. *url* / Safe search selected with a parameter in the URL. *header* / Safe search selected by search header (i.e. youtube.edu).		
charset	Search engine charset.	option	-

Parameter	Description	Type	Size
	Option / **Description** *utf-8* / UTF-8 encoding. *gb2312* / 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
<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 qos-profile on page 1498
- config wireless-controller log on page 1407
- config wireless-controller client-info on page 1510
- config wireless-controller ble-profile on page 1421
- config wireless-controller wtp-group on page 1496
- config wireless-controller hotspot20 anqp-ip-address-type on page 1359
- config wireless-controller vap-status on page 1511
- config wireless-controller address on page 1504
- config wireless-controller hotspot20 hs-profile on page 1368
- config wireless-controller hotspot20 anqp-nai-realm on page 1356
- config wireless-controller hotspot20 icon on page 1365
- config wireless-controller region on page 1413
- config wireless-controller wtp-profile on page 1423
- config wireless-controller utm-profile on page 1503
- config wireless-controller addrgrp on page 1505
- config wireless-controller hotspot20 anqp-network-auth-type on page 1354
- config wireless-controller snmp on page 1505
- config wireless-controller hotspot20 h2qp-wan-metric on page 1361
- config wireless-controller spectral-info on page 1511
- config wireless-controller hotspot20 anqp-3gpp-cellular on page 1359
- config wireless-controller hotspot20 h2qp-conn-capability on page 1362
- config wireless-controller wtp on page 1475
- config wireless-controller setting on page 1400
- config wireless-controller hotspot20 anqp-venue-name on page 1354
- config wireless-controller wlchanlistlic on page 1510
- config wireless-controller wag-profile on page 1502
- config wireless-controller hotspot20 h2qp-osu-provider on page 1366
- config wireless-controller hotspot20 anqp-roaming-consortium on page 1355
- config wireless-controller wids-profile on page 1414
- config wireless-controller scan on page 1509
- config wireless-controller ap-status on page 1509
- config wireless-controller hotspot20 h2qp-operator-name on page 1360
- config wireless-controller rf-analysis on page 1511
- config wireless-controller inter-controller on page 1350
- config wireless-controller global on page 1351
- config wireless-controller bonjour-profile on page 1412
- config wireless-controller vap on page 1375
- config wireless-controller vap-group on page 1414
- config wireless-controller wtp-status on page 1510

- config wireless-controller status on page 1510
- config wireless-controller timers on page 1399
- config wireless-controller hotspot20 qos-map on page 1367

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
inter-controller-mode	Configure inter-controller mode .	option	-

Option	Description
disable	Disable inter-controller mode.
l2-roaming	Enable layer 2 roaming support between inter-controllers.
1+1	Enable 1+1 fast failover mode.

inter-controller-key	Secret key for inter-controller communications.	password	Not Specified
inter-controller-pri	Configure inter-controller's priority .	option	-

Option	Description
primary	Primary fast failover mode.
secondary	Secondary fast failover mode.

Parameter	Description	Type	Size
fast-failover-max	Maximum number of retransmissions for fast failover HA messages between peer wireless controllers .	integer	Minimum value: 3 Maximum value: 64
fast-failover-wait	Minimum wait time before an AP transitions from secondary controller to primary controller .	integer	Minimum value: 10 Maximum value: 86400

config inter-controller-peer

Parameter	Description	Type	Size
peer-ip	Peer wireless controller's IP address.	ipv4-address	Not Specified
peer-port	Port used by the wireless controller's for inter-controller communications .	integer	Minimum value: 1024 Maximum value: 49150
peer-priority	Peer wireless controller's priority .	option	-

Option	Description
primary	Primary fast failover mode.
secondary	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 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
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	-

Option	Description
enable	Enable WTP image download at join time.
disable	Disable WTP image download at join time.

Parameter	Description	Type	Size
max-retransmit	Maximum number of tunnel packet retransmissions .	integer	Minimum value: 0 Maximum value: 64
control-message-offload	Configure CAPWAP control message data channel offload.	option	-

Option	Description
ebp-frame	Ekahau blink protocol (EBP) frames.
aeroscout-tag	AeroScout tag.
ap-list	Rogue AP list.
sta-list	Rogue STA list.
sta-cap-list	STA capability list.
stats	WTP, radio, VAP, and STA statistics.
aeroscout-mu	AeroScout Mobile Unit (MU) report.
sta-health	STA health log.

Parameter	Description	Type	Size
data-ethernet-II	Configure the wireless controller to use Ethernet II or 802.3 frames with 802.3 data tunnel mode .	option	-

Option	Description
enable	Use Ethernet II frames with 802.3 data tunnel mode.

Parameter	Description	Type	Size
	Option **Description** *disable* 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** **Description** *enable* Enable calculating the CAPWAP transmit hash. *disable* Disable calculating the CAPWAP transmit hash.	option	-
mesh-eth-type	Mesh Ethernet identifier included in backhaul packets .	integer	Minimum value: 8755 Maximum value: 8755
fiapp-eth-type	Ethernet type for Fortinet Inter-Access Point Protocol .	integer	Minimum value: 5252 Maximum value: 5252
discovery-mc-addr	Multicast IP address for AP discovery .	ipv4-address-multicast	Not Specified
max-clients	Maximum number of clients that can connect simultaneously .	integer	Minimum value: 0 Maximum value: 4294967295
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
ipsec-base-ip	Base IP address for IPsec VPN tunnels between the access points and the wireless controller .	ipv4-address	Not Specified
wtp-share	Enable/disable sharing of WTPs between VDOMs. **Option** **Description** *enable* WTP can be shared between all VDOMs. *disable* WTP can be used only in its own VDOM.	option	-
ap-log-server	Enable/disable configuring APs or FortiAPs to send log messages to a syslog server .	option	-

Parameter	Description	Type	Size
	Option: *enable* — Enable AP log server. Option: *disable* — Disable AP log server.		
ap-log-server-ip	IP address that APs or FortiAPs send log messages to.	ipv4-address	Not Specified
ap-log-server-port	Port that APs or FortiAPs send log messages to.	integer	Minimum value: 0 Maximum value: 65535

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
lang	Language code.	string	Maximum length: 3
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
auth-type	Network authentication type.	option	-

Option	Description
acceptance-of-terms	Acceptance of terms and conditions.
online-enrollment	Online enrollment supported.
http-redirection	HTTP and HTTPS redirection.
dns-redirection	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
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
```

config nai-list

Parameter	Description	Type	Size
encoding	Enable/disable format in accordance with IETF RFC 4282.	option	-

Option	Description
disable	Disable format in accordance with IETF RFC 4282.
enable	Enable format in accordance with IETF RFC 4282.

Parameter	Description	Type	Size
nai-realm	Configure NAI realms (delimited by a semi-colon character).	string	Maximum length: 255

config eap-method

Parameter	Description	Type	Size
method	EAP method type.	option	-

Parameter	Description	Type	Size

Option	Description
eap-identity	Identity.
eap-md5	MD5.
eap-tls	TLS.
eap-ttls	TTLS.
eap-peap	PEAP.
eap-sim	SIM.
eap-aka	AKA.
eap-aka-prime	AKA'.

config auth-param

Parameter	Description	Type	Size
id	ID of authentication parameter.	option	-

Option	Description
non-eap-inner-auth	Non-EAP inner authentication type.
inner-auth-eap	Inner authentication EAP method type.
credential	Credential type.
tunneled-credential	Tunneled EAP method credential type.

val	Value of authentication parameter.	option	-

Option	Description
eap-identity	EAP Identity.
eap-md5	EAP MD5.
eap-tls	EAP TLS.
eap-ttls	EAP TTLS.
eap-peap	EAP PEAP.
eap-sim	EAP SIM.
eap-aka	EAP AKA.
eap-aka-prime	EAP AKA'.

Parameter	Description	Type	Size

Option	Description
non-eap-pap	Non EAP PAP.
non-eap-chap	Non EAP CHAP.
non-eap-mschap	Non EAP MSCHAP.
non-eap-mschapv2	Non EAP MSCHAPV2.
cred-sim	Credential SIM.
cred-usim	Credential USIM.
cred-nfc	Credential NFC secure element.
cred-hardware-token	Credential hardware token.
cred-softoken	Credential softoken.
cred-certificate	Credential certificate.
cred-user-pwd	Credential username password.
cred-none	Credential none.
cred-vendor-specific	Credential vendor specific.
tun-cred-sim	Tunneled credential SIM.
tun-cred-usim	Tunneled credential USIM.
tun-cred-nfc	Tunneled credential NFC secure element.
tun-cred-hardware-token	Tunneled credential hardware token.
tun-cred-softoken	Tunneled credential softoken.
tun-cred-certificate	Tunneled credential certificate.
tun-cred-user-pwd	Tunneled credential username password.
tun-cred-anonymous	Tunneled credential anonymous.
tun-cred-vendor-specific	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
mcc	Mobile country code.	string	Maximum length: 3
mnc	Mobile network code.	string	Maximum length: 3

config wireless-controller hotspot20 anqp-ip-address-type

Configure IP address type availability.

```
config wireless-controller hotspot20 anqp-ip-address-type
   Description: Configure IP address type availability.
   edit <name>
      set 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
ipv6-address-type	IPv6 address type.	option	-

Option	Description
not-available	Address type not available.
available	Address type available.

Parameter	Description	Type	Size
	Option / **Description** *not-known* / Availability of the address type not known.		
ipv4-address-type	IPv4 address type.	option	-
	Option / **Description** *not-available* / Address type not available. *public* / Public IPv4 address available. *port-restricted* / Port-restricted IPv4 address available. *single-NATed-private* / Single NATed private IPv4 address available. *double-NATed-private* / Double NATed private IPv4 address available. *port-restricted-and-single-NATed* / Port-restricted IPv4 address and single NATed IPv4 address available. *port-restricted-and-double-NATed* / Port-restricted IPv4 address and double NATed IPv4 address available. *not-known* / 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
lang	Language code.	string	Maximum length: 3
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
link-status	Link status.	option	-

Option	Description
up	Link up.
down	Link down.
in-test	Link in test state.

Parameter	Description	Type	Size
symmetric-wan-link	WAN link symmetry.	option	-

Option	Description
symmetric	Symmetric WAN link (uplink and downlink speeds are the same).
asymmetric	Asymmetric WAN link (uplink and downlink speeds are not the same).

Parameter	Description	Type	Size
link-at-capacity	Link at capacity.	option	-

Parameter	Description	Type	Size
	Option: *enable* — Link at capacity (not allow additional mobile devices to associate). Option: *disable* — Link not at capacity (allow additional mobile devices to associate).		
uplink-speed	Uplink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295
downlink-speed	Downlink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295
uplink-load	Uplink load.	integer	Minimum value: 0 Maximum value: 255
downlink-load	Downlink load.	integer	Minimum value: 0 Maximum value: 255
load-measurement-duration	Load measurement duration (in tenths of a second).	integer	Minimum value: 0 Maximum value: 65535

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
icmp-port	Set ICMP port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
ftp-port	Set FTP port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
ssh-port	Set SSH port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
http-port	Set HTTP port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
tls-port	Set TLS VPN (HTTPS) port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
pptp-vpn-port	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
voip-tcp-port	Set VoIP TCP port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
voip-udp-port	Set VoIP UDP port service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
ikev2-port	Set IKEv2 port service for IPsec VPN status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
ikev2-xx-port	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.	option	-

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	The port may or may not be open for communication.

Parameter	Description	Type	Size
esp-port	Set ESP port service (used by IPsec VPNs) status.	option	-

Parameter	Description	Type	Size

Option	Description
closed	The port is not open for communication.
open	The port is open for communication.
unknown	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
lang	Language code.	string	Maximum length: 3
file	Icon file.	string	Maximum length: 255
type	Icon type.	option	-

Option	Description
bmp	BMP image.
gif	GIF image.
jpeg	JPEG image.
png	PNG image.
tiff	TIFF image.

Parameter	Description	Type	Size
width	Icon width.	integer	Minimum value: 1 Maximum value: 65535
height	Icon height.	integer	Minimum value: 1 Maximum value: 65535

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
server-uri	Server URI.	string	Maximum length: 255
osu-method	OSU method list.	option	-

Parameter	Description	Type	Size
	Option: Description *oma-dm*: OMA DM. *soap-xml-spp*: SOAP XML SPP. *reserved*: Reserved.		
osu-nai	OSU NAI.	string	Maximum length: 255
icon	OSU provider icon.	string	Maximum length: 35

config friendly-name

Parameter	Description	Type	Size
lang	Language code.	string	Maximum length: 3
friendly-name	OSU provider friendly name.	string	Maximum length: 252

config service-description

Parameter	Description	Type	Size
lang	Language code.	string	Maximum length: 3
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
dscp	DSCP value.	integer	Minimum value: 0 Maximum value: 63
up	User priority.	integer	Minimum value: 0 Maximum value: 7

config dscp-range

Parameter	Description	Type	Size
up	User priority.	integer	Minimum value: 0 Maximum value: 7
low	DSCP low value.	integer	Minimum value: 0 Maximum value: 63
high	DSCP high value.	integer	Minimum value: 0 Maximum value: 63

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 l2tif [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
access-network-type	Access network type.	option	-

Option	Description
private-network	Private network.
private-network-with-guest-access	Private network with guest access.
chargeable-public-network	Chargeable public network.
free-public-network	Free public network.
personal-device-network	Personal devices network.

Parameter	Description	Type	Size
	Option **Description** *emergency-services-only-network* Emergency services only network. *test-or-experimental* Test or experimental. *wildcard* Wildcard.		
access-network-internet	Enable/disable connectivity to the Internet.	option	-
	Option **Description** *enable* Enable connectivity to the Internet. *disable* Disable connectivity to the Internet.		
access-network-asra	Enable/disable additional step required for access (ASRA).	option	-
	Option **Description** *enable* Enable additional step required for access (ASRA). *disable* Disable additional step required for access (ASRA).		
access-network-esr	Enable/disable emergency services reachable (ESR).	option	-
	Option **Description** *enable* Enable emergency services reachable (ESR). *disable* Disable emergency services reachable (ESR).		
access-network-uesa	Enable/disable unauthenticated emergency service accessible (UESA).	option	-
	Option **Description** *enable* Enable unauthenticated emergency service accessible (UESA). *disable* Disable unauthenticated emergency service accessible (UESA).		
venue-group	Venue group.	option	-
	Option **Description** *unspecified* Unspecified.		

Parameter	Description	Type	Size
	Option / **Description** *assembly* / Assembly. *business* / Business. *educational* / Educational. *factory* / Factory and industrial. *institutional* / Institutional. *mercantile* / Mercantile. *residential* / Residential. *storage* / Storage. *utility* / Utility and miscellaneous. *vehicular* / Vehicular. *outdoor* / Outdoor.		
venue-type	Venue type.	option	-
	Option / **Description** *unspecified* / Unspecified. *arena* / Arena. *stadium* / Stadium. *passenger-terminal* / Passenger terminal. *amphitheater* / Amphitheater. *amusement-park* / Amusement park. *place-of-worship* / Place of worship. *convention-center* / Convention center. *library* / Library. *museum* / Museum. *restaurant* / Restaurant. *theater* / Theater.		

Parameter	Description	Type	Size

Option	Description
bar	Bar.
coffee-shop	Coffee shop.
zoo-or-aquarium	Zoo or aquarium.
emergency-center	Emergency coordination center.
doctor-office	Doctor or dentist office.
bank	Bank.
fire-station	Fire station.
police-station	Police station.
post-office	Post office.
professional-office	Professional office.
research-facility	Research and development facility.
attorney-office	Attorney office.
primary-school	Primary school.
secondary-school	Secondary school.
university-or-college	University or college.
factory	Factory.
hospital	Hospital.
long-term-care-facility	Long term care facility.
rehab-center	Alcohol and drug rehabilitation center.
group-home	Group home.
prison-or-jail	Prison or jail.
retail-store	Retail store.
grocery-market	Grocery market.
auto-service-station	Auto service station.
shopping-mall	Shopping mall.

Parameter	Description	Type	Size
	Option / **Description** *gas-station* — Gas station. *private* — Private residence. *hotel-or-motel* — Hotel or motel. *dormitory* — Dormitory. *boarding-house* — Boarding house. *automobile* — Automobile or truck. *airplane* — Airplane. *bus* — Bus. *ferry* — Ferry. *ship-or-boat* — Ship or boat. *train* — Train. *motor-bike* — Motor bike. *muni-mesh-network* — Muni mesh network. *city-park* — City park. *rest-area* — Rest area. *traffic-control* — Traffic control. *bus-stop* — Bus stop. *kiosk* — Kiosk.		
hessid	Homogeneous extended service set identifier (HESSID).	mac-address	Not Specified
proxy-arp	Enable/disable Proxy ARP.	option	-
	Option / **Description** *enable* — Enable Proxy ARP. *disable* — Disable Proxy ARP.		
l2tif	Enable/disable Layer 2 traffic inspection and filtering.	option	-
	Option / **Description** *enable* — Enable Layer 2 traffic inspection and filtering.		

Parameter	Description	Type	Size
	Option / **Description** *disable* / Disable Layer 2 traffic inspection and filtering.		
pame-bi	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	option	-
	Option / **Description** *disable* / Disable Pre-Association Message Exchange BSSID Independent (PAME-BI). *enable* / Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).		
anqp-domain-id	ANQP Domain ID .	integer	Minimum value: 0 Maximum value: 65535
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: 4000
gas-fragmentation-limit	GAS fragmentation limit .	integer	Minimum value: 512 Maximum value: 4096
dgaf	Enable/disable downstream group-addressed forwarding (DGAF).	option	-
	Option / **Description** *enable* / Enable downstream group-addressed forwarding (DGAF). *disable* / Disable downstream group-addressed forwarding (DGAF).		
deauth-request-timeout	Deauthentication request timeout (in seconds).	integer	Minimum value: 30 Maximum value: 120
wnm-sleep-mode	Enable/disable wireless network management (WNM) sleep mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable wireless network management (WNM) sleep mode. *disable* / Disable wireless network management (WNM) sleep mode.		
bss-transition	Enable/disable basic service set (BSS) transition Support.	option	-
	Option / **Description** *enable* / Enable basic service set (BSS) transition support. *disable* / 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
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 voice-enterprise [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 eapol-key-retries [disable|enable]
   set tkip-counter-measure [enable|disable]
   set external-web {string}
   set external-web-format [auto-detect|no-query-string|...]
   set external-logout {string}
   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 acct-interim-interval {integer}
   set local-standalone [enable|disable]
   set local-standalone-nat [enable|disable]
   set ip {ipv4-classnet-host}
   set dhcp-lease-time {integer}
   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 {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 mpsk [enable|disable]
set mpsk-concurrent-clients {integer}
config mpsk-key
   Description: List of multiple PSK entries.
   edit <key-name>
      set passphrase {password}
      set concurrent-clients {string}
      set comment {var-string}
      set mpsk-schedules <name1>, <name2>, ...
   next
end
set split-tunneling [enable|disable]
set vlanid {integer}
set vlan-auto [enable|disable]
set dynamic-vlan [enable|disable]
set captive-portal-radius-server {string}
set captive-portal-radius-secret {password}
set captive-portal-macauth-radius-server {string}
set captive-portal-macauth-radius-secret {password}
set captive-portal-ac-name {string}
set captive-portal-session-timeout-interval {integer}
set multicast-rate [0|6000|...]
set multicast-enhance [enable|disable]
set broadcast-suppression {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 vlan-pooling [wtp-group|round-robin|...]
config vlan-pool
   Description: VLAN pool.
   edit <id>
      set wtp-group {string}
   next
end
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 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 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
   next
end
```

config wireless-controller vap

Parameter	Description	Type	Size
fast-roaming	Enable/disable fast-roaming, or pre-authentication, where supported by clients .	option	-

Option	Description
enable	Enable fast-roaming, or pre-authentication.
disable	Disable fast-roaming, or pre-authentication.

Parameter	Description	Type	Size
external-fast-roaming	Enable/disable fast roaming or pre-authentication with external APs not managed by the FortiGate .	option	-

Option	Description
enable	Enable fast roaming or pre-authentication with external APs.
disable	Disable fast roaming or pre-authentication with external APs.

Parameter	Description	Type	Size
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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable mesh backhaul. *disable* / Disable mesh backhaul.		
atf-weight	Airtime weight in percentage .	integer	Minimum value: 0 Maximum value: 100
max-clients	Maximum number of clients that can connect simultaneously to the VAP .	integer	Minimum value: 0 Maximum value: 4294967295
max-clients-ap	Maximum number of clients that can connect simultaneously to the VAP per AP radio .	integer	Minimum value: 0 Maximum value: 4294967295
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
broadcast-ssid	Enable/disable broadcasting the SSID .	option	-
	Option / **Description** *enable* / Enable broadcasting the SSID. *disable* / Disable broadcasting the SSID.		
security	Security mode for the wireless interface .	option	-
	Option / **Description** *open* / Open. *captive-portal* / Captive portal. *wep64* / WEP 64-bit. *wep128* / WEP 128-bit. *wpa-personal* / WPA/WPA2 personal.		

Parameter	Description	Type	Size

Option	Description
wpa-personal+captive-portal	WPA/WPA2 personal with captive portal.
wpa-enterprise	WPA/WPA2 enterprise.
wpa-only-personal	WPA personal.
wpa-only-personal+captive-portal	WPA personal with captive portal.
wpa-only-enterprise	WPA enterprise.
wpa2-only-personal	WPA2 personal.
wpa2-only-personal+captive-portal	WPA2 personal with captive portal.
wpa2-only-enterprise	WPA2 enterprise.
wpa3-enterprise	WPA3 enterprise.
wpa3-sae	WPA3 SAE.
wpa3-sae-transition	WPA3 SAE transition.
owe	Opportunistic wireless encryption.
osen	OSEN.

pmf	Protected Management Frames .	option	-

Option	Description
disable	Disable PMF completely.
enable	Enable PMF but deny clients without PMF.
optional	Enable PMF and allow clients without PMF.

pmf-assoc-comeback-timeout	Protected Management Frames .	integer	Minimum value: 1 Maximum value: 20
pmf-sa-query-retry-timeout	Protected Management Frames .	integer	Minimum value: 1 Maximum value: 5

Parameter	Description	Type	Size
okc	Enable/disable Opportunistic Key Caching .	option	-

Option	Description
disable	Disable Opportunistic Key Caching (OKC).
enable	Enable Opportunistic Key Caching (OKC).

Parameter	Description	Type	Size
voice-enterprise	Enable/disable 802.11k and 802.11v assisted Voice-Enterprise roaming .	option	-

Option	Description
disable	Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.
enable	Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.

Parameter	Description	Type	Size
fast-bss-transition	Enable/disable 802.11r Fast BSS Transition .	option	-

Option	Description
disable	Disable 802.11r Fast BSS Transition (FT).
enable	Enable 802.11r Fast BSS Transition (FT).

Parameter	Description	Type	Size
ft-mobility-domain	Mobility domain identifier in FT .	integer	Minimum value: 1 Maximum value: 65535
ft-r0-key-lifetime	Lifetime of the PMK-R0 key in FT, 1-65535 minutes.	integer	Minimum value: 1 Maximum value: 65535
ft-over-ds	Enable/disable FT over the Distribution System (DS).	option	-

Option	Description
disable	Disable FT over the Distribution System (DS).
enable	Enable FT over the Distribution System (DS).

Parameter	Description	Type	Size
sae-groups	SAE-Groups.	option	-

Option	Description
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.

Parameter	Description	Type	Size
owe-groups	OWE-Groups.	option	-

Option	Description
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.

Parameter	Description	Type	Size
owe-transition	Enable/disable OWE transition mode support.	option	-

Option	Description
disable	Disable OWE transition mode support.
enable	Enable OWE transition mode support.

Parameter	Description	Type	Size
owe-transition-ssid	OWE transition mode peer SSID.	string	Maximum length: 32
eapol-key-retries	Enable/disable retransmission of EAPOL-Key frames .	option	-

Option	Description
disable	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).
enable	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).

Parameter	Description	Type	Size
tkip-counter-measure	Enable/disable TKIP counter measure.	option	-

Option	Description
enable	Enable TKIP counter measure.
disable	Disable TKIP counter measure.

Parameter	Description	Type	Size
external-web	URL of external authentication web server.	string	Maximum length: 127
external-web-format	URL query parameter detection .	option	-

Option	Description
auto-detect	Automatically detect if "external-web" URL has any query parameter.
no-query-string	"external-web" URL does not have any query parameter.

Parameter	Description	Type	Size
	Option / **Description** *partial-query-string* — "external-web" URL has some query parameters.		
external-logout	URL of external authentication logout server.	string	Maximum length: 127
mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-
	Option / **Description** *enable* — Enable MAC authentication bypass. *disable* — Disable MAC authentication bypass.		
radius-mac-auth	Enable/disable RADIUS-based MAC authentication of clients .	option	-
	Option / **Description** *enable* — Enable RADIUS-based MAC authentication. *disable* — 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	-
	Option / **Description** *psk* — Use a single Pre-shard Key (PSK) to authenticate all users. *radius* — Use a RADIUS server to authenticate clients. *usergroup* — Use a firewall usergroup to authenticate clients.		
encrypt	Encryption protocol to use (only available when security is set to a WPA type).	option	-
	Option / **Description** *TKIP* — Use TKIP encryption. *AES* — Use AES encryption. *TKIP-AES* — Use TKIP and AES encryption.		

Parameter	Description	Type	Size
keyindex	WEP key index .	integer	Minimum value: 1 Maximum value: 4
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
acct-interim-interval	WiFi RADIUS accounting interim interval .	integer	Minimum value: 60 Maximum value: 86400
local-standalone	Enable/disable AP local standalone .	option	-

Option	Description
enable	Enable AP local standalone.
disable	Disable AP local standalone.

local-standalone-nat	Enable/disable AP local standalone NAT mode.	option	-

Option	Description
enable	Enable AP local standalone NAT mode.
disable	Disable AP local standalone NAT mode.

ip	IP address and subnet mask for the local standalone NAT subnet.	ipv4-classnet-host	Not Specified
dhcp-lease-time	DHCP lease time in seconds for NAT IP address.	integer	Minimum value: 300 Maximum value: 8640000
local-bridging	Enable/disable bridging of wireless and Ethernet interfaces on the FortiAP .	option	-

Option	Description
enable	Enable AP local VAP to Ethernet bridging.
disable	Disable AP local VAP to Ethernet bridging.

Parameter	Description	Type	Size
local-lan	Allow/deny traffic destined for a Class A, B, or C private IP address .	option	-

Option	Description
allow	Allow traffic destined for a Class A, B, or C private IP address.
deny	Deny traffic destined for a Class A, B, or C private IP address.

local-authentication	Enable/disable AP local authentication.	option	-

Option	Description
enable	Enable AP local authentication.
disable	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	-

Option	Description
auth	Portal for authentication.
auth+disclaimer	Portal for authentication and disclaimer.
disclaimer	Portal for disclaimer.
email-collect	Portal for email collection.
cmcc	Portal for CMCC.
cmcc-macauth	Portal for CMCC and MAC authentication.
auth-mac	Portal for authentication and MAC authentication.
external-auth	Portal for external portal authentication.

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

Parameter	Description	Type	Size
security-redirect-url	Optional URL for redirecting users after they pass captive portal authentication.	string	Maximum length: 127
intra-vap-privacy	Enable/disable blocking communication between clients on the same SSID .	option	-

Option	Description
enable	Enable intra-SSID privacy.
disable	Disable intra-SSID privacy.

Parameter	Description	Type	Size
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	-

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.

Parameter	Description	Type	Size
high-efficiency	Enable/disable 802.11ax high efficiency .	option	-

Option	Description
enable	Enable 802.11ax high efficiency.
disable	Disable 802.11ax high efficiency.

Parameter	Description	Type	Size
target-wake-time	Enable/disable 802.11ax target wake time .	option	-

Option	Description
enable	Enable 802.11ax target wake time.
disable	Disable 802.11ax target wake time.

Parameter	Description	Type	Size
mpsk	Enable/disable multiple PSK authentication.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable multiple PSK authentication *disable* / Disable multiple PSK authentication		
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
split-tunneling	Enable/disable split tunneling .	option	-
	Option / **Description** *enable* / Enable split tunneling. *disable* / Disable split tunneling.		
vlanid	Optional VLAN ID.	integer	Minimum value: 0 Maximum value: 4094
vlan-auto	Enable/disable automatic management of SSID VLAN interface.	option	-
	Option / **Description** *enable* / Enable automatic management of SSID VLAN interface. *disable* / Disable automatic management of SSID VLAN interface.		
dynamic-vlan	Enable/disable dynamic VLAN assignment.	option	-
	Option / **Description** *enable* / Enable dynamic VLAN assignment. *disable* / Disable dynamic VLAN assignment.		
captive-portal-radius-server	Captive portal RADIUS server domain name or IP address.	string	Maximum length: 63
captive-portal-radius-secret	Secret key to access the RADIUS server.	password	Not Specified
captive-portal-macauth-radius-server	Captive portal external RADIUS server domain name or IP address.	string	Maximum length: 63

Parameter	Description	Type	Size
captive-portal-macauth-radius-secret	Secret key to access the macauth RADIUS server.	password	Not Specified
captive-portal-ac-name	Local-bridging captive portal ac-name.	string	Maximum length: 35
captive-portal-session-timeout-interval	Session timeout interval .	integer	Minimum value: 0 Maximum value: 864000
multicast-rate	Multicast rate .	option	-

Option	Description
0	Use the default multicast rate.
6000	6 Mbps.
12000	12 Mbps.
24000	24 Mbps.

multicast-enhance	Enable/disable converting multicast to unicast to improve performance .	option	-

Option	Description
enable	Enable multicast enhancement.
disable	Disable multicast enhancement.

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	-

Option	Description
dhcp-up	Suppress broadcast uplink DHCP messages.
dhcp-down	Suppress broadcast downlink DHCP messages.
dhcp-starvation	Suppress broadcast DHCP starvation req messages.
dhcp-ucast	Convert downlink broadcast DHCP messages to unicast messages.
arp-known	Suppress broadcast ARP for known wireless clients.
arp-unknown	Suppress broadcast ARP for unknown wireless clients.
arp-reply	Suppress broadcast ARP reply from wireless clients.

Parameter	Description	Type	Size
	Option / **Description** *arp-poison* / Suppress ARP poison messages from wireless clients. *arp-proxy* / Reply ARP requests for wireless clients as a proxy. *netbios-ns* / Suppress NetBIOS name services packets with UDP port 137. *netbios-ds* / Suppress NetBIOS datagram services packets with UDP port 138. *ipv6* / Suppress IPv6 packets. *all-other-mc* / Suppress all other multicast messages. *all-other-bc* / Suppress all other broadcast messages.		
me-disable-thresh	Disable multicast enhancement when this many clients are receiving multicast traffic.	integer	Minimum value: 2 Maximum value: 256
mu-mimo	Enable/disable Multi-user MIMO .	option	-
	Option / **Description** *enable* / Enable Multi-user MIMO. *disable* / Disable Multi-user MIMO.		
probe-resp-suppression	Enable/disable probe response suppression .	option	-
	Option / **Description** *enable* / Enable probe response suppression. *disable* / Disable probe response suppression.		
probe-resp-threshold	Minimum signal level/threshold in dBm required for the AP response to probe requests .	string	Maximum length: 7
radio-sensitivity	Enable/disable software radio sensitivity .	option	-
	Option / **Description** *enable* / Enable software radio sensitivity. *disable* / Disable software radio sensitivity.		
quarantine	Enable/disable station quarantine .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable station quarantine. *disable* / 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
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
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	-
	Option / **Description** *wtp-group* / Enable VLAN pooling with VLAN assignment by wtp-group. *round-robin* / Enable VLAN pooling with round-robin VLAN assignment. *hash* / Enable VLAN pooling with hash-based VLAN assignment. *disable* / Disable VLAN pooling.		
dhcp-option82-insertion	Enable/disable DHCP option 82 insert .	option	-
	Option / **Description** *enable* / Enable DHCP option 82 insert. *disable* / Disable DHCP option 82 insert.		
dhcp-option82-circuit-id-insertion	Enable/disable DHCP option 82 circuit-id insert .	option	-
	Option / **Description** *style-1* / ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s". *style-2* / ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx". *disable* / Disable DHCP option 82 circuit-id insert.		

Parameter	Description	Type	Size
dhcp-option82-remote-id-insertion	Enable/disable DHCP option 82 remote-id insert .	option	-

Option	Description
style-1	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.
disable	Disable DHCP option 82 remote-id insert.

Parameter	Description	Type	Size
ptk-rekey	Enable/disable PTK rekey for WPA-Enterprise security.	option	-

Option	Description
enable	Enable PTK rekey for WPA-Enterprise security.
disable	Disable PTK rekey for WPA-Enterprise security.

Parameter	Description	Type	Size
ptk-rekey-intv	PTK rekey interval .	integer	Minimum value: 1800 Maximum value: 864000
gtk-rekey	Enable/disable GTK rekey for WPA security.	option	-

Option	Description
enable	Enable GTK rekey for WPA security.
disable	Disable GTK rekey for WPA security.

Parameter	Description	Type	Size
gtk-rekey-intv	GTK rekey interval .	integer	Minimum value: 1800 Maximum value: 864000
eap-reauth	Enable/disable EAP re-authentication for WPA-Enterprise security.	option	-

Option	Description
enable	Enable EAP re-authentication for WPA-Enterprise security.
disable	Disable EAP re-authentication for WPA-Enterprise security.

Parameter	Description	Type	Size
eap-reauth-intv	EAP re-authentication interval .	integer	Minimum value: 1800 Maximum value: 864000

Parameter	Description	Type	Size
qos-profile	Quality of service profile name.	string	Maximum length: 35
hotspot20-profile	Hotspot 2.0 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
tunnel-fallback-interval	The time interval for secondary tunnel to fall back to primary tunnel .	integer	Minimum value: 0 Maximum value: 65535
rates-11a	Allowed data rates for 802.11a.	option	-

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.

Parameter	Description	Type	Size

Option	Description
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.
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.

Parameter	Description	Type	Size
	Option **Description** *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. *mcs3/1* Data rate for MCS index 3 with 1 spatial stream. *mcs4/1* Data rate for MCS index 4 with 1 spatial stream. *mcs5/1* Data rate for MCS index 5 with 1 spatial stream. *mcs6/1* Data rate for MCS index 6 with 1 spatial stream. *mcs7/1* Data rate for MCS index 7 with 1 spatial stream. *mcs8/2* Data rate for MCS index 8 with 2 spatial streams. *mcs9/2* Data rate for MCS index 9 with 2 spatial streams. *mcs10/2* Data rate for MCS index 10 with 2 spatial streams. *mcs11/2* Data rate for MCS index 11 with 2 spatial streams. *mcs12/2* Data rate for MCS index 12 with 2 spatial streams. *mcs13/2* Data rate for MCS index 13 with 2 spatial streams. *mcs14/2* Data rate for MCS index 14 with 2 spatial streams. *mcs15/2* Data rate for MCS index 15 with 2 spatial streams.		
rates-11n-ss34	Allowed data rates for 802.11n with 3 or 4 spatial streams.	option	-

Parameter	Description	Type	Size

Option	Description
mcs16/3	Data rate for MCS index 16 with 3 spatial streams.
mcs17/3	Data rate for MCS index 17 with 3 spatial streams.
mcs18/3	Data rate for MCS index 18 with 3 spatial streams.
mcs19/3	Data rate for MCS index 19 with 3 spatial streams.
mcs20/3	Data rate for MCS index 20 with 3 spatial streams.
mcs21/3	Data rate for MCS index 21 with 3 spatial streams.
mcs22/3	Data rate for MCS index 22 with 3 spatial streams.
mcs23/3	Data rate for MCS index 23 with 3 spatial streams.
mcs24/4	Data rate for MCS index 24 with 4 spatial streams.
mcs25/4	Data rate for MCS index 25 with 4 spatial streams.
mcs26/4	Data rate for MCS index 26 with 4 spatial streams.
mcs27/4	Data rate for MCS index 27 with 4 spatial streams.
mcs28/4	Data rate for MCS index 28 with 4 spatial streams.
mcs29/4	Data rate for MCS index 29 with 4 spatial streams.
mcs30/4	Data rate for MCS index 30 with 4 spatial streams.
mcs31/4	Data rate for MCS index 31 with 4 spatial streams.

rates-11ac-ss12	Allowed data rates for 802.11ac/ax 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.
mcs3/1	Data rate for MCS index 3 with 1 spatial stream.
mcs4/1	Data rate for MCS index 4 with 1 spatial stream.
mcs5/1	Data rate for MCS index 5 with 1 spatial stream.
mcs6/1	Data rate for MCS index 6 with 1 spatial stream.
mcs7/1	Data rate for MCS index 7 with 1 spatial stream.
mcs8/1	Data rate for MCS index 8 with 1 spatial stream.

Parameter	Description	Type	Size

Option	Description
mcs9/1	Data rate for MCS index 9 with 1 spatial stream.
mcs10/1	Data rate for MCS index 10 with 1 spatial stream.
mcs11/1	Data rate for MCS index 11 with 1 spatial stream.
mcs0/2	Data rate for MCS index 0 with 2 spatial streams.
mcs1/2	Data rate for MCS index 1 with 2 spatial streams.
mcs2/2	Data rate for MCS index 2 with 2 spatial streams.
mcs3/2	Data rate for MCS index 3 with 2 spatial streams.
mcs4/2	Data rate for MCS index 4 with 2 spatial streams.
mcs5/2	Data rate for MCS index 5 with 2 spatial streams.
mcs6/2	Data rate for MCS index 6 with 2 spatial streams.
mcs7/2	Data rate for MCS index 7 with 2 spatial streams.
mcs8/2	Data rate for MCS index 8 with 2 spatial streams.
mcs9/2	Data rate for MCS index 9 with 2 spatial streams.
mcs10/2	Data rate for MCS index 10 with 2 spatial streams.
mcs11/2	Data rate for MCS index 11 with 2 spatial streams.

rates-11ac-ss34	Allowed data rates for 802.11ac/ax with 3 or 4 spatial streams.	option	-

Option	Description
mcs0/3	Data rate for MCS index 0 with 3 spatial streams.
mcs1/3	Data rate for MCS index 1 with 3 spatial streams.
mcs2/3	Data rate for MCS index 2 with 3 spatial streams.
mcs3/3	Data rate for MCS index 3 with 3 spatial streams.
mcs4/3	Data rate for MCS index 4 with 3 spatial streams.
mcs5/3	Data rate for MCS index 5 with 3 spatial streams.
mcs6/3	Data rate for MCS index 6 with 3 spatial streams.
mcs7/3	Data rate for MCS index 7 with 3 spatial streams.
mcs8/3	Data rate for MCS index 8 with 3 spatial streams.
mcs9/3	Data rate for MCS index 9 with 3 spatial streams.

Parameter	Description	Type	Size
	Option / **Description** *mcs10/3* — Data rate for MCS index 10 with 3 spatial streams. *mcs11/3* — Data rate for MCS index 11 with 3 spatial streams. *mcs0/4* — Data rate for MCS index 0 with 4 spatial streams. *mcs1/4* — Data rate for MCS index 1 with 4 spatial streams. *mcs2/4* — Data rate for MCS index 2 with 4 spatial streams. *mcs3/4* — Data rate for MCS index 3 with 4 spatial streams. *mcs4/4* — Data rate for MCS index 4 with 4 spatial streams. *mcs5/4* — Data rate for MCS index 5 with 4 spatial streams. *mcs6/4* — Data rate for MCS index 6 with 4 spatial streams. *mcs7/4* — Data rate for MCS index 7 with 4 spatial streams. *mcs8/4* — Data rate for MCS index 8 with 4 spatial streams. *mcs9/4* — Data rate for MCS index 9 with 4 spatial streams. *mcs10/4* — Data rate for MCS index 10 with 4 spatial streams. *mcs11/4* — Data rate for MCS index 11 with 4 spatial streams.		
utm-profile	UTM profile name.	string	Maximum length: 35
address-group	Address group ID.	string	Maximum length: 35
mac-filter	Enable/disable MAC filtering to block wireless clients by mac address. **Option** / **Description** *enable* — Enable MAC filtering. *disable* — Disable MAC filtering.	option	-
mac-filter-policy-other	Allow or block clients with MAC addresses that are not in the filter list. **Option** / **Description** *allow* — Allow clients with MAC addresses that are not in the filter list. *deny* — Block clients with MAC addresses that are not in the filter list.	option	-

config portal-message-overrides

Parameter	Description	Type	Size
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 mpsk-key

Parameter	Description	Type	Size
passphrase	WPA Pre-shared key.	password	Not Specified
concurrent-clients	Number of clients that can connect using this pre-shared key.	string	Maximum length: 15
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 vlan-pool

Parameter	Description	Type	Size
wtp-group	WTP group name.	string	Maximum length: 35

config mac-filter-list

Parameter	Description	Type	Size
mac	MAC address.	mac-address	Not Specified
mac-filter-policy	Deny or allow the client with this MAC address.	option	-

Parameter	Description	Type	Size

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-cleanup {integer}
   set ble-scan-report-intv {integer}
end
```

config wireless-controller timers

Parameter	Description	Type	Size
echo-interval	Time between echo requests sent by the managed WTP, AP, or FortiAP .	integer	Minimum value: 1 Maximum value: 255
discovery-interval	Time between discovery requests .	integer	Minimum value: 2 Maximum value: 180
client-idle-timeout	Time after which a client is considered idle and times out .	integer	Minimum value: 20 Maximum value: 3600
rogue-ap-log	Time between logging rogue AP messages if periodic rogue AP logging is configured .	integer	Minimum value: 0 Maximum value: 1440

Parameter	Description	Type	Size
fake-ap-log	Time between recording logs about fake APs if periodic fake AP logging is configured .	integer	Minimum value: 1 Maximum value: 1440
sta-stats-interval	Time between running client .	integer	Minimum value: 1 Maximum value: 255
vap-stats-interval	Time between running Virtual Access Point .	integer	Minimum value: 1 Maximum value: 255
radio-stats-interval	Time between running radio reports .	integer	Minimum value: 1 Maximum value: 255
sta-capability-interval	Time between running station capability reports .	integer	Minimum value: 1 Maximum value: 255
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
ipsec-intf-cleanup	Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected .	integer	Minimum value: 30 Maximum value: 3600
ble-scan-report-intv	Time between running Bluetooth Low Energy .	integer	Minimum value: 10 Maximum value: 3600

config wireless-controller setting

VDOM wireless controller configuration.

```
config wireless-controller setting
   Description: VDOM wireless controller configuration.
   set account-id {string}
   set country [NA|AL|...]
   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 darrp-optimize {integer}
   set darrp-optimize-schedules <name1>, <name2>, ...
end
```

config wireless-controller setting

Parameter	Description	Type	Size
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	-

Option	Description
NA	NO_COUNTRY_SET
AL	ALBANIA
DZ	ALGERIA
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

Parameter	Description	Type	Size

Option	Description
BO	BOLIVIA
BA	BOSNIA AND HERZEGOVINA
BR	BRAZIL
BN	BRUNEI DARUSSALAM
BG	BULGARIA
KH	CAMBODIA
CF	CENTRAL AFRICA REPUBLIC
CL	CHILE
CN	CHINA
CO	COLOMBIA
CR	COSTA RICA
HR	CROATIA
CY	CYPRUS
CZ	CZECH REPUBLIC
DK	DENMARK
DO	DOMINICAN REPUBLIC
EC	ECUADOR
EG	EGYPT
SV	EL SALVADOR
EE	ESTONIA
FI	FINLAND
FR	FRANCE
GE	GEORGIA
DE	GERMANY
GR	GREECE
GL	GREENLAND
GD	GRENADA
GU	GUAM
GT	GUATEMALA

Parameter	Description	Type	Size

Option	Description
HT	HAITI
HN	HONDURAS
HK	HONG KONG
HU	HUNGARY
IS	ICELAND
IN	INDIA
ID	INDONESIA
IR	IRAN
IE	IRELAND
IL	ISRAEL
IT	ITALY
JM	JAMAICA
JO	JORDAN
KZ	KAZAKHSTAN
KE	KENYA
KP	NORTH KOREA
KR	KOREA REPUBLIC
KW	KUWAIT
LV	LATVIA
LB	LEBANON
LI	LIECHTENSTEIN
LT	LITHUANIA
LU	LUXEMBOURG
MO	MACAU SAR
MK	MACEDONIA, FYRO
MY	MALAYSIA
MT	MALTA
MX	MEXICO
MC	MONACO

Parameter	Description	Type	Size

Option	Description
MA	MOROCCO
MZ	MOZAMBIQUE
MM	MYANMAR
NP	NEPAL
NL	NETHERLANDS
AN	NETHERLANDS ANTILLES
AW	ARUBA
NZ	NEW ZEALAND
NO	NORWAY
OM	OMAN
PK	PAKISTAN
PA	PANAMA
PG	PAPUA NEW GUINEA
PY	PARAGUAY
PE	PERU
PH	PHILIPPINES
PL	POLAND
PT	PORTUGAL
PR	PUERTO RICO
QA	QATAR
RO	ROMANIA
RU	RUSSIA
RW	RWANDA
SA	SAUDI ARABIA
RS	REPUBLIC OF SERBIA
ME	MONTENEGRO
SG	SINGAPORE
SK	SLOVAKIA
SI	SLOVENIA

Parameter	Description	Type	Size
	Option / **Description** *ZA* SOUTH AFRICA *ES* SPAIN *LK* SRI LANKA *SE* SWEDEN *SD* SUDAN *CH* SWITZERLAND *SY* SYRIAN ARAB REPUBLIC *TW* TAIWAN *TZ* TANZANIA *TH* THAILAND *TT* TRINIDAD AND TOBAGO *TN* TUNISIA *TR* TURKEY *AE* UNITED ARAB EMIRATES *UA* UKRAINE *GB* UNITED KINGDOM *US* UNITED STATES2 *PS* UNITED STATES (PUBLIC SAFETY) *UY* URUGUAY *UZ* UZBEKISTAN *VE* VENEZUELA *VN* VIET NAM *YE* YEMEN *ZB* ZAMBIA *ZW* ZIMBABWE *JP* JAPAN14 *CA* CANADA2		
duplicate-ssid	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Allow VAPs to use the same SSID name in the same VDOM. *disable* / Do not allow VAPs to use the same SSID name in the same VDOM.		
fapc-compatibility	Enable/disable FAP-C series compatibility.	option	-
	Option / **Description** *enable* / Enable FAP-C series compatibility. *disable* / Disable FAP-C series compatibility.		
wfa-compatibility	Enable/disable WFA compatibility.	option	-
	Option / **Description** *enable* / Enable Wi-Fi Alliance Certification compatibility. *disable* / Disable Wi-Fi Alliance Certification compatibility.		
phishing-ssid-detect	Enable/disable phishing SSID detection.	option	-
	Option / **Description** *enable* / Enable phishing SSID detection. *disable* / Disable phishing SSID detection.		
fake-ssid-action	Actions taken for detected fake SSID.	option	-
	Option / **Description** *log* / Write logs for detected fake SSID. *suppress* / Suppress detected fake SSID.		
darrp-optimize	Time for running Dynamic Automatic Radio Resource Provisioning .	integer	Minimum value: 0 Maximum value: 86400
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35

config offending-ssid

Parameter	Description	Type	Size
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	-

Option	Description
log	Generate logs for detected offending SSID.
suppress	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
status	Enable/disable wireless event logging.	option	-

Option	Description
enable	Enable wireless event logging.
disable	Disable wireless event logging.

addrgrp-log	Lowest severity level to log address group message.	option	-

Parameter	Description	Type	Size
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
ble-log	Lowest severity level to log BLE detection message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
clb-log	Lowest severity level to log client load balancing message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		

Parameter	Description	Type	Size
dhcp-starv-log	Lowest severity level to log DHCP starvation event message.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

led-sched-log	Lowest severity level to log LED schedule event message.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

radio-event-log	Lowest severity level to log radio event message.	option	-

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.

Parameter	Description	Type	Size
	Option / **Description** *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
rogue-event-log	Lowest severity level to log rogue AP event message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
sta-event-log	Lowest severity level to log station event message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
sta-locate-log	Lowest severity level to log station locate message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level.		

Parameter	Description	Type	Size
	Option / **Description** *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
wids-log	Lowest severity level to log WIDS message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		
wtp-event-log	Lowest severity level to log WTP event message.	option	-
	Option / **Description** *emergency* — Emergency level. *alert* — Alert level. *critical* — Critical level. *error* — Error level. *warning* — Warning level. *notification* — Notification level. *information* — Information level. *debug* — Debug level.		

config wireless-controller bonjour-profile

Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connnect 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 connnect 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
comment	Comment.	string	Maximum length: 63

config policy-list

Parameter	Description	Type	Size
description	Description.	string	Maximum length: 63
from-vlan	VLAN ID from which the Bonjour service is advertised .	string	Maximum length: 63
to-vlan	VLAN ID to which the Bonjour service is made available .	string	Maximum length: 63
services	Bonjour services for the VLAN connecting to the Bonjour network.	option	-

Option	Description
all	All services.
airplay	AirPlay.

Parameter	Description	Type	Size

Option	Description
afp	AFP (Apple File Sharing).
bit-torrent	BitTorrent.
ftp	FTP.
ichat	iChat.
itunes	iTunes.
printers	Printers.
samba	Samba.
scanners	Scanners.
ssh	SSH.
chromecast	ChromeCast.

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
comments	Comments.	string	Maximum length: 1027
grayscale	Region image grayscale.	option	-

Option	Description
enable	Enable region image grayscale.
disable	Disable region image grayscale.

Parameter	Description	Type	Size
opacity	Region image opacity .	integer	Minimum value: 0 Maximum value: 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
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-unknown-src-thresh {integer}
   next
end
```

config wireless-controller wids-profile

Parameter	Description	Type	Size
comment	Comment.	string	Maximum length: 63
sensor-mode	Scan nearby WiFi stations .	option	-

Option	Description
disable	Disable the scan.
foreign	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.
both	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	-

Parameter	Description	Type	Size
	Option **Description** *disable* Disable rogue AP detection. *enable* Enable rogue AP detection.		
ap-bgscan-period	Period of time between background scans .	integer	Minimum value: 60 Maximum value: 3600
ap-bgscan-intv	Period of time between scanning two channels .	integer	Minimum value: 1 Maximum value: 600
ap-bgscan-duration	Listening time on a scanning channel .	integer	Minimum value: 10 Maximum value: 1000
ap-bgscan-idle	Waiting time for channel inactivity before scanning this channel .	integer	Minimum value: 0 Maximum value: 1000
ap-bgscan-report-intv	Period of time between background scan reports .	integer	Minimum value: 15 Maximum value: 600
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
ap-scan-passive	Enable/disable passive scanning. Enable means do not send probe request on any channels .	option	-
	Option **Description** *enable* Passive scanning on all channels. *disable* Passive scanning only on DFS channels.		

Parameter	Description	Type	Size
ap-scan-threshold	Minimum signal level/threshold in dBm required for the AP to report detected rogue AP .	string	Maximum length: 7
ap-auto-suppress	Enable/disable on-wire rogue AP auto-suppression .	option	-

Option	Description
enable	Enable on-wire rogue AP auto-suppression.
disable	Disable on-wire rogue AP auto-suppression.

wireless-bridge	Enable/disable wireless bridge detection .	option	-

Option	Description
enable	Enable wireless bridge detection.
disable	Disable wireless bridge detection.

deauth-broadcast	Enable/disable broadcasting de-authentication detection .	option	-

Option	Description
enable	Enable broadcast de-authentication detection.
disable	Disable broadcast de-authentication detection.

null-ssid-probe-resp	Enable/disable null SSID probe response detection .	option	-

Option	Description
enable	Enable null SSID probe resp detection.
disable	Disable null SSID probe resp detection.

long-duration-attack	Enable/disable long duration attack detection based on user configured threshold .	option	-

Option	Description
enable	Enable long duration attack detection.
disable	Disable long duration attack detection.

long-duration-thresh	Threshold value for long duration attack detection .	integer	Minimum value: 1000 Maximum value: 32767

Parameter	Description	Type	Size
invalid-mac-oui	Enable/disable invalid MAC OUI detection.	option	-

Option	Description
enable	Enable invalid MAC OUI detection.
disable	Disable invalid MAC OUI detection.

weak-wep-iv	Enable/disable weak WEP IV .	option	-

Option	Description
enable	Enable weak WEP IV detection.
disable	Disable weak WEP IV detection.

auth-frame-flood	Enable/disable authentication frame flooding detection .	option	-

Option	Description
enable	Enable authentication frame flooding detection.
disable	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
auth-flood-thresh	The threshold value for authentication frame flooding.	integer	Minimum value: 1 Maximum value: 100
assoc-frame-flood	Enable/disable association frame flooding detection .	option	-

Option	Description
enable	Enable association frame flooding detection.
disable	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

Parameter	Description	Type	Size
assoc-flood-thresh	The threshold value for association frame flooding.	integer	Minimum value: 1 Maximum value: 100
spoofed-deauth	Enable/disable spoofed de-authentication attack detection .	option	-

Option	Description
enable	Enable spoofed de-authentication attack detection.
disable	Disable spoofed de-authentication attack detection.

asleap-attack	Enable/disable asleap attack detection .	option	-

Option	Description
enable	Enable asleap attack detection.
disable	Disable asleap attack detection.

eapol-start-flood	Enable/disable EAPOL-Start flooding .	option	-

Option	Description
enable	Enable EAPOL-Start flooding detection.
disable	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
eapol-start-intv	The detection interval for EAPOL-Start flooding .	integer	Minimum value: 1 Maximum value: 3600
eapol-logoff-flood	Enable/disable EAPOL-Logoff flooding .	option	-

Option	Description
enable	Enable EAPOL-Logoff flooding detection.
disable	Disable EAPOL-Logoff flooding detection.

Parameter	Description	Type	Size
eapol-logoff-thresh	The threshold value for EAPOL-Logoff flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100
eapol-logoff-intv	The detection interval for EAPOL-Logoff flooding .	integer	Minimum value: 1 Maximum value: 3600
eapol-succ-flood	Enable/disable EAPOL-Success flooding .	option	-

Option	Description
enable	Enable EAPOL-Success flooding detection.
disable	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
eapol-succ-intv	The detection interval for EAPOL-Success flooding .	integer	Minimum value: 1 Maximum value: 3600
eapol-fail-flood	Enable/disable EAPOL-Failure flooding .	option	-

Option	Description
enable	Enable EAPOL-Failure flooding detection.
disable	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
eapol-fail-intv	The detection interval for EAPOL-Failure flooding .	integer	Minimum value: 1 Maximum value: 3600
eapol-pre-succ-flood	Enable/disable premature EAPOL-Success flooding .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable premature EAPOL-Success flooding detection. *disable* / Disable premature EAPOL-Success flooding detection.		
eapol-pre-succ-thresh	The threshold value for premature EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100
eapol-pre-succ-intv	The detection interval for premature EAPOL-Success flooding .	integer	Minimum value: 1 Maximum value: 3600
eapol-pre-fail-flood	Enable/disable premature EAPOL-Failure flooding .	option	-
	Option / **Description** *enable* / Enable premature EAPOL-Failure flooding detection. *disable* / 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
eapol-pre-fail-intv	The detection interval for premature EAPOL-Failure flooding .	integer	Minimum value: 1 Maximum value: 3600
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

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
comment	Comment.	string	Maximum length: 63
advertising	Advertising type.	option	-

Option	Description
ibeacon	iBeacon advertising.
eddystone-uid	Eddystone UID advertising.
eddystone-url	Eddystone URL advertising.

ibeacon-uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 63
major-id	Major ID.	integer	Minimum value: 0 Maximum value: 65535
minor-id	Minor ID.	integer	Minimum value: 0 Maximum value: 65535
eddystone-namespace	Eddystone namespace ID.	string	Maximum length: 10
eddystone-instance	Eddystone instance ID.	string	Maximum length: 6
eddystone-url	Eddystone URL.	string	Maximum length: 127
txpower	Transmit power level .	option	-

Option	Description
0	Transmit power level 0 (-21 dBm)
1	Transmit power level 1 (-18 dBm)

Parameter	Description	Type	Size
	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
ble-scanning	Enable/disable Bluetooth Low Energy (BLE) scanning. **Option** / **Description** *enable* — Enable BLE scanning. *disable* — Disable BLE scanning.	option	-

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 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}
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 [NA|AL|...]
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|...]
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 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 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 power-level {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 channel-utilization [enable|disable]
    set spectrum-analysis [enable|disable]
    set wids-profile {string}
    set darrp [enable|disable]
    set max-clients {integer}
    set max-distance {integer}
    set frequency-handoff [enable|disable]
    set ap-handoff [enable|disable]
    set vap-all [enable|disable]
    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 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 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 power-level {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 channel-utilization [enable|disable]
    set spectrum-analysis [enable|disable]
    set wids-profile {string}
    set darrp [enable|disable]
    set max-clients {integer}
    set max-distance {integer}
    set frequency-handoff [enable|disable]
    set ap-handoff [enable|disable]
    set vap-all [enable|disable]
    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 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 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 power-level {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 channel-utilization [enable|disable]
    set spectrum-analysis [enable|disable]
    set wids-profile {string}
    set darrp [enable|disable]
    set max-clients {integer}
    set max-distance {integer}
    set frequency-handoff [enable|disable]
    set ap-handoff [enable|disable]
    set vap-all [enable|disable]
    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 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 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 power-level {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 channel-utilization [enable|disable]
    set spectrum-analysis [enable|disable]
    set wids-profile {string}
    set darrp [enable|disable]
    set max-clients {integer}
    set max-distance {integer}
    set frequency-handoff [enable|disable]
```

```
        set ap-handoff [enable|disable]
        set vap-all [enable|disable]
        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-mmu-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]
  next
end
```

config wireless-controller wtp-profile

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
control-message-offload	Enable/disable CAPWAP control message data channel offload.	option	-

Option	Description
ebp-frame	Ekahau blink protocol (EBP) frames.

Parameter	Description	Type	Size
	Option / **Description** *aeroscout-tag* / AeroScout tag. *ap-list* / Rogue AP list. *sta-list* / Rogue STA list. *sta-cap-list* / STA capability list. *stats* / WTP, radio, VAP, and STA statistics. *aeroscout-mu* / AeroScout Mobile Unit (MU) report. *sta-health* / STA health log.		
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	-
	Option / **Description** *wan-lan* / Enable using a WAN port as a LAN port. *wan-only* / Disable using a WAN port as a LAN port.		
energy-efficient-ethernet	Enable/disable use of energy efficient Ethernet on WTP.	option	-
	Option / **Description** *enable* / Enable use of energy efficient Ethernet on WTP. *disable* / Disable use of energy efficient Ethernet on WTP.		
led-state	Enable/disable use of LEDs on WTP .	option	-
	Option / **Description** *enable* / Enable use of LEDs on WTP. *disable* / Disable use of LEDs on WTP.		
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	-

Parameter	Description	Type	Size
	Option / **Description** *clear-text* / Clear Text Data Channel. *dtls-enabled* / DTLS Enabled Data Channel. *ipsec-vpn* / IPsec VPN Data Channel.		
dtls-in-kernel	Enable/disable data channel DTLS in kernel.	option	-
	Option / **Description** *enable* / Enable data channel DTLS in kernel. *disable* / Disable data channel DTLS in kernel.		
max-clients	Maximum number of stations .	integer	Minimum value: 0 Maximum value: 4294967295
handoff-rssi	Minimum received signal strength indicator .	integer	Minimum value: 20 Maximum value: 30
handoff-sta-thresh	Threshold value for AP handoff.	integer	Minimum value: 0 Maximum value: 4294967295
handoff-roaming	Enable/disable client load balancing during roaming to avoid roaming delay .	option	-
	Option / **Description** *enable* / Enable handoff roaming. *disable* / Disable handoff roaming.		
ap-country	Country in which this WTP, FortiAP or AP will operate .	option	-
	Option / **Description** *NA* / NO_COUNTRY_SET *AL* / ALBANIA *DZ* / ALGERIA		

Parameter	Description	Type	Size

Option	Description
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
BO	BOLIVIA
BA	BOSNIA AND HERZEGOVINA
BR	BRAZIL
BN	BRUNEI DARUSSALAM
BG	BULGARIA
KH	CAMBODIA
CF	CENTRAL AFRICA REPUBLIC
CL	CHILE
CN	CHINA
CO	COLOMBIA
CR	COSTA RICA
HR	CROATIA
CY	CYPRUS
CZ	CZECH REPUBLIC
DK	DENMARK
DO	DOMINICAN REPUBLIC

Parameter	Description	Type	Size

Option	Description
EC	ECUADOR
EG	EGYPT
SV	EL SALVADOR
EE	ESTONIA
FI	FINLAND
FR	FRANCE
GE	GEORGIA
DE	GERMANY
GR	GREECE
GL	GREENLAND
GD	GRENADA
GU	GUAM
GT	GUATEMALA
HT	HAITI
HN	HONDURAS
HK	HONG KONG
HU	HUNGARY
IS	ICELAND
IN	INDIA
ID	INDONESIA
IR	IRAN
IE	IRELAND
IL	ISRAEL
IT	ITALY
JM	JAMAICA
JO	JORDAN
KZ	KAZAKHSTAN
KE	KENYA
KP	NORTH KOREA

Parameter	Description	Type	Size

Option	Description
KR	KOREA REPUBLIC
KW	KUWAIT
LV	LATVIA
LB	LEBANON
LI	LIECHTENSTEIN
LT	LITHUANIA
LU	LUXEMBOURG
MO	MACAU SAR
MK	MACEDONIA, FYRO
MY	MALAYSIA
MT	MALTA
MX	MEXICO
MC	MONACO
MA	MOROCCO
MZ	MOZAMBIQUE
MM	MYANMAR
NP	NEPAL
NL	NETHERLANDS
AN	NETHERLANDS ANTILLES
AW	ARUBA
NZ	NEW ZEALAND
NO	NORWAY
OM	OMAN
PK	PAKISTAN
PA	PANAMA
PG	PAPUA NEW GUINEA
PY	PARAGUAY
PE	PERU
PH	PHILIPPINES

Parameter	Description	Type	Size

Option	Description
PL	POLAND
PT	PORTUGAL
PR	PUERTO RICO
QA	QATAR
RO	ROMANIA
RU	RUSSIA
RW	RWANDA
SA	SAUDI ARABIA
RS	REPUBLIC OF SERBIA
ME	MONTENEGRO
SG	SINGAPORE
SK	SLOVAKIA
SI	SLOVENIA
ZA	SOUTH AFRICA
ES	SPAIN
LK	SRI LANKA
SE	SWEDEN
SD	SUDAN
CH	SWITZERLAND
SY	SYRIAN ARAB REPUBLIC
TW	TAIWAN
TZ	TANZANIA
TH	THAILAND
TT	TRINIDAD AND TOBAGO
TN	TUNISIA
TR	TURKEY
AE	UNITED ARAB EMIRATES
UA	UKRAINE
GB	UNITED KINGDOM

Parameter	Description	Type	Size
	Option / **Description** *US* — UNITED STATES2 *PS* — UNITED STATES (PUBLIC SAFETY) *UY* — URUGUAY *UZ* — UZBEKISTAN *VE* — VENEZUELA *VN* — VIET NAM *YE* — YEMEN *ZB* — ZAMBIA *ZW* — ZIMBABWE *JP* — JAPAN14 *CA* — CANADA2		
ip-fragment-preventing	Method. **Option** / **Description** *tcp-mss-adjust* — TCP maximum segment size adjustment. *icmp-unreachable* — Drop packet and send ICMP Destination Unreachable	option	-
tun-mtu-uplink	The maximum transmission unit .	integer	Minimum value: 576 Maximum value: 1500
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel .	integer	Minimum value: 576 Maximum value: 1500
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel. **Option** / **Description** *tunnel* — Split tunneling ACL list traffic will be tunnel. *local* — Split tunneling ACL list traffic will be local NATed.	option	-

Parameter	Description	Type	Size
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL .	option	-

Option	Description
enable	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.
disable	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.

allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-

Option	Description
https	HTTPS access.
ssh	SSH access.
snmp	SNMP access.

login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP .	option	-

Option	Description
yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.
default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.
no	Do not change the managed WTP, FortiAP or AP's administrator password.

login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified
lldp	Enable/disable Link Layer Discovery Protocol .	option	-

Option	Description
enable	Enable LLDP.
disable	Disable LLDP.

poe-mode	Set the WTP, FortiAP, or AP's PoE mode.	option	-

Option	Description
auto	Automatically detect the PoE mode.

Parameter	Description	Type	Size
	Option / **Description** *8023af* / Use 802.3af PoE mode. *8023at* / Use 802.3at PoE mode. *power-adapter* / Use the power adapter to control the PoE mode.		
ext-info-enable	Enable/disable station/VAP/radio extension information.	option	-
	Option / **Description** *enable* / Enable station/VAP/radio extension information. *disable* / Disable station/VAP/radio extension information.		

config platform

Parameter	Description	Type	Size
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	-
	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.		

Parameter	Description	Type	Size

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
	Option / **Description** *231E* FAP231E. *S221E* FAPS221E. *S223E* FAPS223E. *321E* FAP321E. *431F* FAP431F. *432F* FAP432F. *433F* FAP433F. *231F* FAP231F. *234F* FAP234F. *23JF* FAP23JF. *U421E* FAPU421EV. *U422EV* FAPU422EV. *U423E* FAPU423EV. *U221EV* FAPU221EV. *U223EV* FAPU223EV. *U24JEV* FAPU24JEV. *U321EV* FAPU321EV. *U323EV* FAPU323EV. *U431F* FAPU431F. *U433F* FAPU433F.		
mode	Configure operation mode of 5G radios .	option	-
	Option / **Description** *single-5G* Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer. *dual-5G* Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.		
ddscan	Enable/disable use of one radio for dedicated dual-band scanning to detect RF characterization and wireless threat management.	option	-

Parameter	Description	Type	Size

Option	Description
enable	Enable dedicated dual-band scan mode.
disable	Disable dedicated dual-band scan mode.

config lan

Parameter	Description	Type	Size
port-mode	LAN port mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15
port1-mode	LAN port 1 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15
port2-mode	LAN port 2 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15

Parameter	Description	Type	Size
port3-mode	LAN port 3 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15
port4-mode	LAN port 4 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15
port5-mode	LAN port 5 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15
port6-mode	LAN port 6 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

Parameter	Description	Type	Size
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15
port7-mode	LAN port 7 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15
port8-mode	LAN port 8 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15

config deny-mac-list

Parameter	Description	Type	Size
mac	A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.	mac-address	Not Specified

config split-tunneling-acl

Parameter	Description	Type	Size
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified

config radio-1

Parameter	Description	Type	Size
mode	Mode of radio 1. Radio 1 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-

Option	Description
disabled	Radio 1 is disabled.
ap	Radio 1 operates as an access point that allows WiFi clients to connect to your network.
monitor	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.
sniffer	Radio 1 operates as a sniffer capturing WiFi frames on air.

band	WiFi band that Radio 1 operates on.	option	-

Option	Description
802.11a	802.11a.
802.11b	802.11b.
802.11g	802.11g/b.
802.11n	802.11n/g/b at 2.4GHz.
802.11n-5G	802.11n/a at 5GHz.
802.11ac	802.11ac/n/a.
802.11ax-5G	802.11ax/ac/n/a at 5GHz.
802.11ax	802.11ax/n/g/b at 2.4GHz.
802.11n,g-only	802.11n/g at 2.4GHz.
802.11g-only	802.11g.
802.11n-only	802.11n at 2.4GHz.
802.11n-5G-only	802.11n at 5GHz.
802.11ac,n-only	802.11ac/n.
802.11ac-only	802.11ac.
802.11ax,ac-only	802.11ax/ac at 5GHz.
802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.
802.11ax-5G-only	802.11ax at 5GHz.
802.11ax,n-only	802.11ax/n at 2.4GHz.

Parameter	Description	Type	Size
	Option **Description** *802.11ax,n,g-only* 802.11ax/n/g at 2.4GHz. *802.11ax-only* 802.11ax at 2.4GHz.		
band-5g-type	WiFi 5G band type.	option	-
	Option **Description** *5g-full* Full 5G band. *5g-high* High 5G band. *5g-low* Low 5G band.		
airtime-fairness	Enable/disable airtime fairness .	option	-
	Option **Description** *enable* Enable airtime fairness (ATF) support. *disable* Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-
	Option **Description** *rtscts* Enable 802.11g protection RTS/CTS mode. *ctsonly* Enable 802.11g protection CTS only mode. *disable* Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-
	Option **Description** *tim* TIM bit for client in power save mode. *ac-vo* Use AC VO priority to send out packets in the power save queue. *no-obss-scan* Do not put OBSS scan IE into beacon and probe response frames. *no-11b-rate* Do not send frame using 11b data rate. *client-rate-follow* 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	-

Parameter	Description	Type	Size

Option	Description
disable	Disable packet transmission optimization.
power-save	Tag client as operating in power save mode if excessive transmit retries occur.
aggr-limit	Set aggregation limit to a lower value when data rate is low.
retry-limit	Set software retry limit to a lower value when data rate is low.
send-bar	Limit transmission of BAR frames.

Parameter	Description	Type	Size
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-

Option	Description
enable	Enable AMSDU support.
disable	Disable AMSDU support.

Parameter	Description	Type	Size
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-

Option	Description
enable	Enable support for both HT20 and HT40 on the same radio.
disable	Disable support for both HT20 and HT40 on the same radio.

Parameter	Description	Type	Size
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-

Option	Description
enable	Enable zero wait DFS
disable	Disable zero wait DFS

Parameter	Description	Type	Size
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
enable	Select the 400 ns short guard interval (Short GI).
disable	Select the 800 ns long guard interval (Long GI).

Parameter	Description	Type	Size
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-

Parameter	Description	Type	Size
	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** **Description** *enable* Enable automatic transmit power adjustment. *disable* Disable automatic transmit power adjustment.	option	-
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
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
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
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535
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

Parameter	Description	Type	Size
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management beacon frame.
disable	Disable sniffer on WiFi management beacon frame.

ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management probe frame.
disable	Enable sniffer on WiFi management probe frame.

ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management other frame.
disable	Disable sniffer on WiFi management other frame.

ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-

Option	Description
enable	Enable sniffer on WiFi control frame.
disable	Disable sniffer on WiFi control frame.

Parameter	Description	Type	Size
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-

Option	Description
enable	Enable sniffer on WiFi data frame
disable	Disable sniffer on WiFi data frame

Parameter	Description	Type	Size
channel-utilization	Enable/disable measuring channel utilization.	option	-

Option	Description
enable	Enable measuring channel utilization.
disable	Disable measuring channel utilization.

Parameter	Description	Type	Size
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
enable	Enable spectrum analysis.
disable	Disable spectrum analysis.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable distributed automatic radio resource provisioning.
disable	Disable distributed automatic radio resource provisioning.

Parameter	Description	Type	Size
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000
frequency-handoff	Enable/disable frequency handoff of clients to other channels .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable frequency handoff. *disable* / Disable frequency handoff.		
ap-handoff	Enable/disable AP handoff of clients to other APs .	option	-
	Option / **Description** *enable* / Enable AP handoff. *disable* / Disable AP handoff.		
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-
	Option / **Description** *enable* / Automatically select tunnel VAPs. *disable* / Manually select VAPs.		
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	-
	Option / **Description** *enable* / Enable WMM call admission control. *disable* / Disable WMM call admission control.		
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable WMM bandwidth admission control.
disable	Disable WMM bandwidth admission control.

bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000

config radio-2

Parameter	Description	Type	Size
mode	Mode of radio 2. Radio 2 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-

Option	Description
disabled	Radio 2 is disabled.
ap	Radio 2 operates as an access point that allows WiFi clients to connect to your network.
monitor	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.
sniffer	Radio 2 operates as a sniffer capturing WiFi frames on air.

band	WiFi band that Radio 2 operates on.	option	-

Option	Description
802.11a	802.11a.
802.11b	802.11b.
802.11g	802.11g/b.
802.11n	802.11n/g/b at 2.4GHz.
802.11n-5G	802.11n/a at 5GHz.
802.11ac	802.11ac/n/a.

Parameter	Description	Type	Size
	Option **Description** *802.11ax-5G* 802.11ax/ac/n/a at 5GHz. *802.11ax* 802.11ax/n/g/b at 2.4GHz. *802.11n,g-only* 802.11n/g at 2.4GHz. *802.11g-only* 802.11g. *802.11n-only* 802.11n at 2.4GHz. *802.11n-5G-only* 802.11n at 5GHz. *802.11ac,n-only* 802.11ac/n. *802.11ac-only* 802.11ac. *802.11ax,ac-only* 802.11ax/ac at 5GHz. *802.11ax,ac,n-only* 802.11ax/ac/n at 5GHz. *802.11ax-5G-only* 802.11ax at 5GHz. *802.11ax,n-only* 802.11ax/n at 2.4GHz. *802.11ax,n,g-only* 802.11ax/n/g at 2.4GHz. *802.11ax-only* 802.11ax at 2.4GHz.		
band-5g-type	WiFi 5G band type.	option	-
	Option **Description** *5g-full* Full 5G band. *5g-high* High 5G band. *5g-low* Low 5G band.		
airtime-fairness	Enable/disable airtime fairness .	option	-
	Option **Description** *enable* Enable airtime fairness (ATF) support. *disable* Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-

Parameter	Description	Type	Size
	Option / **Description** *rtscts* / Enable 802.11g protection RTS/CTS mode. *ctsonly* / Enable 802.11g protection CTS only mode. *disable* / Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-
	Option / **Description** *tim* / TIM bit for client in power save mode. *ac-vo* / Use AC VO priority to send out packets in the power save queue. *no-obss-scan* / Do not put OBSS scan IE into beacon and probe response frames. *no-11b-rate* / Do not send frame using 11b data rate. *client-rate-follow* / 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** *disable* / Disable packet transmission optimization. *power-save* / Tag client as operating in power save mode if excessive transmit retries occur. *aggr-limit* / Set aggregation limit to a lower value when data rate is low. *retry-limit* / Set software retry limit to a lower value when data rate is low. *send-bar* / Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-
	Option / **Description** *enable* / Enable AMSDU support. *disable* / Disable AMSDU support.		
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable support for both HT20 and HT40 on the same radio. *disable* / Disable support for both HT20 and HT40 on the same radio.		
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-
	Option / **Description** *enable* / Enable zero wait DFS *disable* / Disable zero wait DFS		
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** *enable* / Select the 400 ns short guard interval (Short GI). *disable* / 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	-
	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	-
	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

Parameter	Description	Type	Size
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
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
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535
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
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management beacon frame.
disable	Disable sniffer on WiFi management beacon frame.

Parameter	Description	Type	Size
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management probe frame.
disable	Enable sniffer on WiFi management probe frame.

Parameter	Description	Type	Size
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management other frame.
disable	Disable sniffer on WiFi management other frame.

Parameter	Description	Type	Size
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-

Option	Description
enable	Enable sniffer on WiFi control frame.
disable	Disable sniffer on WiFi control frame.

Parameter	Description	Type	Size
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-

Option	Description
enable	Enable sniffer on WiFi data frame
disable	Disable sniffer on WiFi data frame

Parameter	Description	Type	Size
channel-utilization	Enable/disable measuring channel utilization.	option	-

Option	Description
enable	Enable measuring channel utilization.
disable	Disable measuring channel utilization.

Parameter	Description	Type	Size
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
enable	Enable spectrum analysis.
disable	Disable spectrum analysis.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable distributed automatic radio resource provisioning.
disable	Disable distributed automatic radio resource provisioning.

Parameter	Description	Type	Size
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000
frequency-handoff	Enable/disable frequency handoff of clients to other channels .	option	-

Option	Description
enable	Enable frequency handoff.
disable	Disable frequency handoff.

Parameter	Description	Type	Size
ap-handoff	Enable/disable AP handoff of clients to other APs .	option	-

Option	Description
enable	Enable AP handoff.
disable	Disable AP handoff.

Parameter	Description	Type	Size
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-

Option	Description
enable	Automatically select tunnel VAPs.
disable	Manually select VAPs.

Parameter	Description	Type	Size
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable WMM call admission control.
disable	Disable WMM call admission control.

Parameter	Description	Type	Size
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60
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	-

Option	Description
enable	Enable WMM bandwidth admission control.
disable	Disable WMM bandwidth admission control.

Parameter	Description	Type	Size
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000

config radio-3

Parameter	Description	Type	Size
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-

Option	Description
disabled	Radio 3 is disabled.
ap	Radio 3 operates as an access point that allows WiFi clients to connect to your network.

Parameter	Description	Type	Size

Option	Description
monitor	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.
sniffer	Radio 3 operates as a sniffer capturing WiFi frames on air.

Parameter	Description	Type	Size
band	WiFi band that Radio 3 operates on.	option	-

Option	Description
802.11a	802.11a.
802.11b	802.11b.
802.11g	802.11g/b.
802.11n	802.11n/g/b at 2.4GHz.
802.11n-5G	802.11n/a at 5GHz.
802.11ac	802.11ac/n/a.
802.11ax-5G	802.11ax/ac/n/a at 5GHz.
802.11ax	802.11ax/n/g/b at 2.4GHz.
802.11n,g-only	802.11n/g at 2.4GHz.
802.11g-only	802.11g.
802.11n-only	802.11n at 2.4GHz.
802.11n-5G-only	802.11n at 5GHz.
802.11ac,n-only	802.11ac/n.
802.11ac-only	802.11ac.
802.11ax,ac-only	802.11ax/ac at 5GHz.
802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.
802.11ax-5G-only	802.11ax at 5GHz.
802.11ax,n-only	802.11ax/n at 2.4GHz.
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.
802.11ax-only	802.11ax at 2.4GHz.

Parameter	Description	Type	Size
band-5g-type	WiFi 5G band type.	option	-

Option	Description
5g-full	Full 5G band.

Parameter	Description	Type	Size
	Option **Description** *5g-high* High 5G band. *5g-low* Low 5G band.		
airtime-fairness	Enable/disable airtime fairness .	option	-
	Option **Description** *enable* Enable airtime fairness (ATF) support. *disable* Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-
	Option **Description** *rtscts* Enable 802.11g protection RTS/CTS mode. *ctsonly* Enable 802.11g protection CTS only mode. *disable* Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-
	Option **Description** *tim* TIM bit for client in power save mode. *ac-vo* Use AC VO priority to send out packets in the power save queue. *no-obss-scan* Do not put OBSS scan IE into beacon and probe response frames. *no-11b-rate* Do not send frame using 11b data rate. *client-rate-follow* 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** *disable* Disable packet transmission optimization. *power-save* Tag client as operating in power save mode if excessive transmit retries occur. *aggr-limit* Set aggregation limit to a lower value when data rate is low.		

Parameter	Description	Type	Size
	Option **Description** *retry-limit* Set software retry limit to a lower value when data rate is low. *send-bar* 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** *enable* Enable AMSDU support. *disable* Disable AMSDU support.		
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-
	Option **Description** *enable* Enable support for both HT20 and HT40 on the same radio. *disable* Disable support for both HT20 and HT40 on the same radio.		
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-
	Option **Description** *enable* Enable zero wait DFS *disable* Disable zero wait DFS		
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** *enable* Select the 400 ns short guard interval (Short GI). *disable* 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	-
	Option **Description** *160MHz* 160 MHz channel width. *80MHz* 80 MHz channel width.		

Parameter	Description	Type	Size
	Option **Description** *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** **Description** *enable* Enable automatic transmit power adjustment. *disable* Disable automatic transmit power adjustment.	option	-
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
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
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
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535
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
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346

Parameter	Description	Type	Size
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management beacon frame.
disable	Disable sniffer on WiFi management beacon frame.

Parameter	Description	Type	Size
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management probe frame.
disable	Enable sniffer on WiFi management probe frame.

Parameter	Description	Type	Size
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management other frame.
disable	Disable sniffer on WiFi management other frame.

Parameter	Description	Type	Size
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-

Option	Description
enable	Enable sniffer on WiFi control frame.
disable	Disable sniffer on WiFi control frame.

Parameter	Description	Type	Size
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable sniffer on WiFi data frame *disable* — Disable sniffer on WiFi data frame		
channel-utilization	Enable/disable measuring channel utilization.	option	-
	Option / **Description** *enable* — Enable measuring channel utilization. *disable* — Disable measuring channel utilization.		
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-
	Option / **Description** *enable* — Enable spectrum analysis. *disable* — Disable spectrum analysis.		
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	-
	Option / **Description** *enable* — Enable distributed automatic radio resource provisioning. *disable* — 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
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000
frequency-handoff	Enable/disable frequency handoff of clients to other channels .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable frequency handoff. *disable* / Disable frequency handoff.		
ap-handoff	Enable/disable AP handoff of clients to other APs .	option	-
	Option / **Description** *enable* / Enable AP handoff. *disable* / Disable AP handoff.		
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-
	Option / **Description** *enable* / Automatically select tunnel VAPs. *disable* / Manually select VAPs.		
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	-
	Option / **Description** *enable* / Enable WMM call admission control. *disable* / Disable WMM call admission control.		
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable WMM bandwidth admission control.
disable	Disable WMM bandwidth admission control.

bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000

config radio-4

Parameter	Description	Type	Size
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-

Option	Description
disabled	Radio 3 is disabled.
ap	Radio 3 operates as an access point that allows WiFi clients to connect to your network.
monitor	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.
sniffer	Radio 3 operates as a sniffer capturing WiFi frames on air.

band	WiFi band that Radio 3 operates on.	option	-

Option	Description
802.11a	802.11a.
802.11b	802.11b.
802.11g	802.11g/b.
802.11n	802.11n/g/b at 2.4GHz.
802.11n-5G	802.11n/a at 5GHz.
802.11ac	802.11ac/n/a.

Parameter	Description	Type	Size
	Option / **Description** *802.11ax-5G* / 802.11ax/ac/n/a at 5GHz. *802.11ax* / 802.11ax/n/g/b at 2.4GHz. *802.11n,g-only* / 802.11n/g at 2.4GHz. *802.11g-only* / 802.11g. *802.11n-only* / 802.11n at 2.4GHz. *802.11n-5G-only* / 802.11n at 5GHz. *802.11ac,n-only* / 802.11ac/n. *802.11ac-only* / 802.11ac. *802.11ax,ac-only* / 802.11ax/ac at 5GHz. *802.11ax,ac,n-only* / 802.11ax/ac/n at 5GHz. *802.11ax-5G-only* / 802.11ax at 5GHz. *802.11ax,n-only* / 802.11ax/n at 2.4GHz. *802.11ax,n,g-only* / 802.11ax/n/g at 2.4GHz. *802.11ax-only* / 802.11ax at 2.4GHz.		
band-5g-type	WiFi 5G band type.	option	-
	Option / **Description** *5g-full* / Full 5G band. *5g-high* / High 5G band. *5g-low* / Low 5G band.		
airtime-fairness	Enable/disable airtime fairness .	option	-
	Option / **Description** *enable* / Enable airtime fairness (ATF) support. *disable* / Disable airtime fairness (ATF) support.		
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-

Parameter	Description	Type	Size
	Option / **Description** *rtscts* / Enable 802.11g protection RTS/CTS mode. *ctsonly* / Enable 802.11g protection CTS only mode. *disable* / Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-
	Option / **Description** *tim* / TIM bit for client in power save mode. *ac-vo* / Use AC VO priority to send out packets in the power save queue. *no-obss-scan* / Do not put OBSS scan IE into beacon and probe response frames. *no-11b-rate* / Do not send frame using 11b data rate. *client-rate-follow* / 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** *disable* / Disable packet transmission optimization. *power-save* / Tag client as operating in power save mode if excessive transmit retries occur. *aggr-limit* / Set aggregation limit to a lower value when data rate is low. *retry-limit* / Set software retry limit to a lower value when data rate is low. *send-bar* / Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients .	option	-
	Option / **Description** *enable* / Enable AMSDU support. *disable* / Disable AMSDU support.		
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable support for both HT20 and HT40 on the same radio. *disable* / Disable support for both HT20 and HT40 on the same radio.		
zero-wait-dfs	Enable/disable zero wait DFS on radio .	option	-
	Option / **Description** *enable* / Enable zero wait DFS *disable* / Disable zero wait DFS		
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** *enable* / Select the 400 ns short guard interval (Short GI). *disable* / 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	-
	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	-
	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

Parameter	Description	Type	Size
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
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
beacon-interval	Beacon interval. The time between beacon frames in msec .	integer	Minimum value: 0 Maximum value: 65535
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
frag-threshold	Maximum packet size that can be sent without fragmentation .	integer	Minimum value: 800 Maximum value: 2346
ap-sniffer-bufsize	Sniffer buffer size .	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer .	integer	Minimum value: 0 Maximum value: 4294967295
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management beacon frame.
disable	Disable sniffer on WiFi management beacon frame.

Parameter	Description	Type	Size
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management probe frame.
disable	Enable sniffer on WiFi management probe frame.

Parameter	Description	Type	Size
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-

Option	Description
enable	Enable sniffer on WiFi management other frame.
disable	Disable sniffer on WiFi management other frame.

Parameter	Description	Type	Size
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame .	option	-

Option	Description
enable	Enable sniffer on WiFi control frame.
disable	Disable sniffer on WiFi control frame.

Parameter	Description	Type	Size
ap-sniffer-data	Enable/disable sniffer on WiFi data frame .	option	-

Option	Description
enable	Enable sniffer on WiFi data frame
disable	Disable sniffer on WiFi data frame

Parameter	Description	Type	Size
channel-utilization	Enable/disable measuring channel utilization.	option	-

Option	Description
enable	Enable measuring channel utilization.
disable	Disable measuring channel utilization.

Parameter	Description	Type	Size
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
enable	Enable spectrum analysis.
disable	Disable spectrum analysis.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable distributed automatic radio resource provisioning.
disable	Disable distributed automatic radio resource provisioning.

Parameter	Description	Type	Size
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients .	integer	Minimum value: 0 Maximum value: 54000
frequency-handoff	Enable/disable frequency handoff of clients to other channels .	option	-

Option	Description
enable	Enable frequency handoff.
disable	Disable frequency handoff.

Parameter	Description	Type	Size
ap-handoff	Enable/disable AP handoff of clients to other APs .	option	-

Option	Description
enable	Enable AP handoff.
disable	Disable AP handoff.

Parameter	Description	Type	Size
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-

Option	Description
enable	Automatically select tunnel VAPs.
disable	Manually select VAPs.

Parameter	Description	Type	Size
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35

Parameter	Description	Type	Size
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	-

Option	Description
enable	Enable WMM call admission control.
disable	Disable WMM call admission control.

call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60
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	-

Option	Description
enable	Enable WMM bandwidth admission control.
disable	Disable WMM bandwidth admission control.

bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000

config lbs

Parameter	Description	Type	Size
ekahau-blink-mode	Enable/disable Ekahau blink mode .	option	-

Option	Description
enable	Enable Ekahau blink mode.
disable	Disable Ekahau blink mode.

ekahau-tag	WiFi frame MAC address or WiFi Tag.	mac-address	Not Specified

Parameter	Description	Type	Size
erc-server-ip	IP address of Ekahau RTLS Controller (ERC).	ipv4-address-any	Not Specified
erc-server-port	Ekahau RTLS Controller (ERC) UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535
aeroscout	Enable/disable AeroScout Real Time Location Service .	option	-

Option	Description
enable	Enable AeroScout support.
disable	Disable AeroScout support.

aeroscout-server-ip	IP address of AeroScout server.	ipv4-address-any	Not Specified
aeroscout-server-port	AeroScout server UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535
aeroscout-mu	Enable/disable AeroScout Mobile Unit .	option	-

Option	Description
enable	Enable AeroScout MU mode support.
disable	Disable AeroScout MU mode support.

aeroscout-ap-mac	Use BSSID or board MAC address as AP MAC address in AeroScout AP messages .	option	-

Option	Description
bssid	Use BSSID as AP MAC address in AeroScout AP messages.
board-mac	Use board MAC address as AP MAC address in AeroScout AP messages.

aeroscout-mmu-report	Enable/disable compounded AeroScout tag and MU report .	option	-

Option	Description
enable	Enable compounded AeroScout tag and MU report.
disable	Disable compounded AeroScout tag and MU report.

Parameter	Description	Type	Size
aeroscout-mu-factor	AeroScout MU mode dilution factor .	integer	Minimum value: 0 Maximum value: 4294967295
aeroscout-mu-timeout	AeroScout MU mode timeout .	integer	Minimum value: 0 Maximum value: 65535
fortipresence	Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network .	option	-

Option	Description
foreign	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.
both	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.
disable	Disable FortiPresence.

fortipresence-server	FortiPresence server IP address.	ipv4-address-any	Not Specified
fortipresence-port	FortiPresence server UDP listening port .	integer	Minimum value: 300 Maximum value: 65535
fortipresence-secret	FortiPresence secret password (max. 16 characters).	password	Not Specified
fortipresence-project	FortiPresence project name .	string	Maximum length: 16
fortipresence-frequency	FortiPresence report transmit frequency .	integer	Minimum value: 5 Maximum value: 65535
fortipresence-rogue	Enable/disable FortiPresence finding and reporting rogue APs.	option	-

Option	Description
enable	Enable FortiPresence finding and reporting rogue APs.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable FortiPresence finding and reporting rogue APs.		
fortipresence-unassoc	Enable/disable FortiPresence finding and reporting unassociated stations.	option	-
	Option **Description** *enable* Enable FortiPresence finding and reporting unassociated stations. *disable* Disable FortiPresence finding and reporting unassociated stations.		
fortipresence-ble	Enable/disable FortiPresence finding and reporting BLE devices.	option	-
	Option **Description** *enable* Enable FortiPresence finding and reporting BLE devices. *disable* Disable FortiPresence finding and reporting BLE devices.		
station-locate	Enable/disable client station locating services for all clients, whether associated or not .	option	-
	Option **Description** *enable* Enable station locating service. *disable* Disable station locating service.		

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 admin [discovered|disable|...]
      set name {string}
      set location {string}
      set region {string}
      set region-x {string}
      set region-y {string}
      set wtp-profile {string}
      set wtp-mode [normal|remote]
      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}
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-analysis [enable|disable]
   set spectrum-analysis [enable|disable]
   set override-txpower [enable|disable]
   set auto-power-level [enable|disable]
   set auto-power-high {integer}
   set auto-power-low {integer}
   set power-level {integer}
   set override-vaps [enable|disable]
   set vap-all [enable|disable]
   set vaps <name1>, <name2>, ...
   set override-channel [enable|disable]
   set channel <chan1>, <chan2>, ...
end
```

```
      config radio-2
         Description: Configuration options for radio 2.
         set override-band [enable|disable]
         set band [802.11a|802.11b|...]
         set override-analysis [enable|disable]
         set spectrum-analysis [enable|disable]
         set override-txpower [enable|disable]
         set auto-power-level [enable|disable]
         set auto-power-high {integer}
         set auto-power-low {integer}
         set power-level {integer}
         set override-vaps [enable|disable]
         set vap-all [enable|disable]
         set vaps <name1>, <name2>, ...
         set override-channel [enable|disable]
         set channel <chan1>, <chan2>, ...
      end
      config radio-3
         Description: Configuration options for radio 3.
         set override-band [enable|disable]
         set band [802.11a|802.11b|...]
         set override-analysis [enable|disable]
         set spectrum-analysis [enable|disable]
         set override-txpower [enable|disable]
         set auto-power-level [enable|disable]
         set auto-power-high {integer}
         set auto-power-low {integer}
         set power-level {integer}
         set override-vaps [enable|disable]
         set vap-all [enable|disable]
         set vaps <name1>, <name2>, ...
         set override-channel [enable|disable]
         set channel <chan1>, <chan2>, ...
      end
      config radio-4
         Description: Configuration options for radio 4.
         set override-band [enable|disable]
         set band [802.11a|802.11b|...]
         set override-analysis [enable|disable]
         set spectrum-analysis [enable|disable]
         set override-txpower [enable|disable]
         set auto-power-level [enable|disable]
         set auto-power-high {integer}
         set auto-power-low {integer}
         set power-level {integer}
         set override-vaps [enable|disable]
         set vap-all [enable|disable]
         set vaps <name1>, <name2>, ...
         set override-channel [enable|disable]
         set channel <chan1>, <chan2>, ...
      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
index	Index .	integer	Minimum value: 0 Maximum value: 4294967295
admin	Configure how the FortiGate operating as a wireless controller discovers and manages this WTP, AP or FortiAP.	option	-

Option	Description
discovered	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.
disable	FortiGate wireless controller is configured to not provide service to this WTP.
enable	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
region-y	Relative vertical region coordinate (between 0 and 1).	string	Maximum length: 15
wtp-profile	WTP profile name to apply to this WTP, AP or FortiAP.	string	Maximum length: 35
wtp-mode	WTP, AP, or FortiAP operating mode; normal or remote. A tunnel mode SSID can be assigned to an AP in normal mode but not remote mode, while a local-bridge mode SSID can be assigned to an AP in either normal mode or remote mode.	option	-

Option	Description
normal	Normal WTP, AP, or FortiAP.
remote	Remote WTP, AP, or FortiAP.

bonjour-profile	Bonjour profile name.	string	Maximum length: 35

Parameter	Description	Type	Size
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	-

Option	Description
enable	Override the WTP profile LED state.
disable	Use the WTP profile LED state.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Allow the LEDs on this FortiAP to light.
disable	Keep the LEDs on this FortiAP off.

Parameter	Description	Type	Size
override-wan-port-mode	Enable/disable overriding the wan-port-mode in the WTP profile.	option	-

Option	Description
enable	Override the WTP profile wan-port-mode.
disable	Use the wan-port-mode in the WTP profile.

Parameter	Description	Type	Size
wan-port-mode	Enable/disable using the FortiAP WAN port as a LAN port.	option	-

Option	Description
wan-lan	Use the FortiAP WAN port as a LAN port.
wan-only	Do not use the WAN port as a LAN port.

Parameter	Description	Type	Size
override-ip-fragment	Enable/disable overriding the WTP profile IP fragment prevention setting.	option	-

Option	Description
enable	Override the WTP profile IP fragment prevention setting.
disable	Use the WTP profile IP fragment prevention setting.

Parameter	Description	Type	Size
ip-fragment-preventing	Method.	option	-

Parameter	Description	Type	Size
	Option / **Description** *tcp-mss-adjust* — TCP maximum segment size adjustment. *icmp-unreachable* — Drop packet and send ICMP Destination Unreachable		
tun-mtu-uplink	The maximum transmission unit .	integer	Minimum value: 576 Maximum value: 1500
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel .	integer	Minimum value: 576 Maximum value: 1500
override-split-tunnel	Enable/disable overriding the WTP profile split tunneling setting.	option	-
	Option / **Description** *enable* — Override the WTP profile split tunneling setting. *disable* — Use the WTP profile split tunneling setting.		
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-
	Option / **Description** *tunnel* — Split tunneling ACL list traffic will be tunnel. *local* — 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	-
	Option / **Description** *enable* — Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL. *disable* — Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
override-lan	Enable to override the WTP profile LAN port setting.	option	-

Parameter	Description	Type	Size
	Option **Description** *enable* Override the WTP profile LAN port setting. *disable* Use the WTP profile LAN port setting.		
override-allowaccess	Enable to override the WTP profile management access configuration.	option	-
	Option **Description** *enable* Override the WTP profile management access configuration. *disable* 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** *https* HTTPS access. *ssh* SSH access. *snmp* SNMP access.		
override-login-passwd-change	Enable to override the WTP profile login-password (administrator password) setting.	option	-
	Option **Description** *enable* Override the WTP profile login-password (administrator password) setting. *disable* 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	-
	Option **Description** *yes* Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password. *default* Keep the managed WTP, FortiAP or AP's administrator password set to the factory default. *no* Do not change the managed WTP, FortiAP or AP's administrator password.		
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified

Parameter	Description	Type	Size
image-download	Enable/disable WTP image download.	option	-

Option	Description
enable	Enable WTP image download at join time.
disable	Disable WTP image download at join time.

Parameter	Description	Type	Size
mesh-bridge-enable	Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.	option	-

Option	Description
default	Use mesh Ethernet bridge local setting on the WTP.
enable	Turn on mesh Ethernet bridge on the WTP.
disable	Turn off mesh Ethernet bridge on the WTP.

Parameter	Description	Type	Size
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
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified

config lan

Parameter	Description	Type	Size
port-mode	LAN port mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

Parameter	Description	Type	Size
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15
port1-mode	LAN port 1 mode.	option	-

Parameter	Description	Type	Size
	Option / **Description** *offline* / Offline. *nat-to-wan* / NAT WTP LAN port to WTP WAN port. *bridge-to-wan* / Bridge WTP LAN port to WTP WAN port. *bridge-to-ssid* / Bridge WTP LAN port to SSID.		
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15
port2-mode	LAN port 2 mode.	option	-
	Option / **Description** *offline* / Offline. *nat-to-wan* / NAT WTP LAN port to WTP WAN port. *bridge-to-wan* / Bridge WTP LAN port to WTP WAN port. *bridge-to-ssid* / Bridge WTP LAN port to SSID.		
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15
port3-mode	LAN port 3 mode.	option	-
	Option / **Description** *offline* / Offline. *nat-to-wan* / NAT WTP LAN port to WTP WAN port. *bridge-to-wan* / Bridge WTP LAN port to WTP WAN port. *bridge-to-ssid* / Bridge WTP LAN port to SSID.		
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15
port4-mode	LAN port 4 mode.	option	-
	Option / **Description** *offline* / Offline. *nat-to-wan* / NAT WTP LAN port to WTP WAN port. *bridge-to-wan* / Bridge WTP LAN port to WTP WAN port. *bridge-to-ssid* / Bridge WTP LAN port to SSID.		

Parameter	Description	Type	Size
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15
port5-mode	LAN port 5 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15
port6-mode	LAN port 6 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15
port7-mode	LAN port 7 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.
bridge-to-wan	Bridge WTP LAN port to WTP WAN port.
bridge-to-ssid	Bridge WTP LAN port to SSID.

port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15
port8-mode	LAN port 8 mode.	option	-

Option	Description
offline	Offline.
nat-to-wan	NAT WTP LAN port to WTP WAN port.

Parameter	Description	Type	Size
	Option / **Description** *bridge-to-wan* / Bridge WTP LAN port to WTP WAN port. *bridge-to-ssid* / Bridge WTP LAN port to SSID.		
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15

config radio-1

Parameter	Description	Type	Size
override-band	Enable to override the WTP profile band setting.	option	-
	Option / **Description** *enable* / Override the WTP profile band setting. *disable* / Use the WTP profile band setting.		
band	WiFi band that Radio 1 operates on.	option	-
	Option / **Description** *802.11a* / 802.11a. *802.11b* / 802.11b. *802.11g* / 802.11g/b. *802.11n* / 802.11n/g/b radio at 2.4GHz band. *802.11n-5G* / 802.11n/a at 5GHz. *802.11n,g-only* / 802.11n/g at 2.4GHz. *802.11g-only* / 802.11g. *802.11n-only* / 802.11n at 2.4GHz. *802.11n-5G-only* / 802.11n at 5GHz. *802.11ac* / 802.11ac/n/a radio. *802.11ac,n-only* / 802.11ac/n. *802.11ac-only* / 802.11ac. *802.11ax-5G* / 802.11ax/ac/n/a at 5GHz. *802.11ax,ac-only* / 802.11ax/ac at 5GHz. *802.11ax,ac,n-only* / 802.11ax/ac/n at 5GHz.		

Parameter	Description	Type	Size

Option	Description
802.11ax-5G-only	802.11ax at 5GHz.
802.11ax	802.11ax/n/g/b at 2.4GHz.
802.11ax,n-only	802.11ax/n at 2.4GHz.
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.
802.11ax-only	802.11ax at 2.4GHz.

override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-

Option	Description
enable	Override the WTP profile spectrum analysis configuration.
disable	Use the WTP profile spectrum analysis configuration.

spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
enable	Enable spectrum analysis.
disable	Disable spectrum analysis.

override-txpower	Enable to override the WTP profile power level configuration.	option	-

Option	Description
enable	Override the WTP profile power level configuration.
disable	Use the WTP profile power level configuration.

auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-

Option	Description
enable	Enable automatic transmit power adjustment.
disable	Disable automatic transmit power adjustment.

Parameter	Description	Type	Size
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
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-

Option	Description
enable	Override WTP profile VAP settings.
disable	Use WTP profile VAP settings.

vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-

Option	Description
enable	Automatically select tunnel VAPs.
disable	Manually select VAPs.

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	-

Option	Description
enable	Override WTP profile channel settings.
disable	Use WTP profile channel settings.

channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3

config radio-2

Parameter	Description	Type	Size
override-band	Enable to override the WTP profile band setting.	option	-

Option	Description
enable	Override the WTP profile band setting.
disable	Use the WTP profile band setting.

Parameter	Description	Type	Size
band	WiFi band that Radio 2 operates on.	option	-

Option	Description
802.11a	802.11a.
802.11b	802.11b.
802.11g	802.11g/b.
802.11n	802.11n/g/b radio at 2.4GHz band.
802.11n-5G	802.11n/a at 5GHz.
802.11n,g-only	802.11n/g at 2.4GHz.
802.11g-only	802.11g.
802.11n-only	802.11n at 2.4GHz.
802.11n-5G-only	802.11n at 5GHz.
802.11ac	802.11ac/n/a radio.
802.11ac,n-only	802.11ac/n.
802.11ac-only	802.11ac.
802.11ax-5G	802.11ax/ac/n/a at 5GHz.
802.11ax,ac-only	802.11ax/ac at 5GHz.
802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.
802.11ax-5G-only	802.11ax at 5GHz.
802.11ax	802.11ax/n/g/b at 2.4GHz.
802.11ax,n-only	802.11ax/n at 2.4GHz.
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.
802.11ax-only	802.11ax at 2.4GHz.

Parameter	Description	Type	Size
override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Override the WTP profile spectrum analysis configuration. *disable* — Use the WTP profile spectrum analysis configuration.		
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-
	Option / **Description** *enable* — Enable spectrum analysis. *disable* — Disable spectrum analysis.		
override-txpower	Enable to override the WTP profile power level configuration.	option	-
	Option / **Description** *enable* — Override the WTP profile power level configuration. *disable* — Use the WTP profile power level configuration.		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-
	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
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100

Parameter	Description	Type	Size
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-

Option	Description
enable	Override WTP profile VAP settings.
disable	Use WTP profile VAP settings.

Parameter	Description	Type	Size
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-

Option	Description
enable	Automatically select tunnel VAPs.
disable	Manually select VAPs.

Parameter	Description	Type	Size
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	-

Option	Description
enable	Override WTP profile channel settings.
disable	Use WTP profile channel settings.

Parameter	Description	Type	Size
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3

config radio-3

Parameter	Description	Type	Size
override-band	Enable to override the WTP profile band setting.	option	-

Option	Description
enable	Override the WTP profile band setting.
disable	Use the WTP profile band setting.

Parameter	Description	Type	Size
band	WiFi band that Radio 3 operates on.	option	-

Option	Description
802.11a	802.11a.

Parameter	Description	Type	Size

Option	Description
802.11b	802.11b.
802.11g	802.11g/b.
802.11n	802.11n/g/b radio at 2.4GHz band.
802.11n-5G	802.11n/a at 5GHz.
802.11n,g-only	802.11n/g at 2.4GHz.
802.11g-only	802.11g.
802.11n-only	802.11n at 2.4GHz.
802.11n-5G-only	802.11n at 5GHz.
802.11ac	802.11ac/n/a radio.
802.11ac,n-only	802.11ac/n.
802.11ac-only	802.11ac.
802.11ax-5G	802.11ax/ac/n/a at 5GHz.
802.11ax,ac-only	802.11ax/ac at 5GHz.
802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.
802.11ax-5G-only	802.11ax at 5GHz.
802.11ax	802.11ax/n/g/b at 2.4GHz.
802.11ax,n-only	802.11ax/n at 2.4GHz.
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.
802.11ax-only	802.11ax at 2.4GHz.

override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-

Option	Description
enable	Override the WTP profile spectrum analysis configuration.
disable	Use the WTP profile spectrum analysis configuration.

spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
enable	Enable spectrum analysis.

Parameter	Description	Type	Size
	Option **Description** *disable* Disable spectrum analysis.		
override-txpower	Enable to override the WTP profile power level configuration.	option	-
	Option **Description** *enable* Override the WTP profile power level configuration. *disable* Use the WTP profile power level configuration.		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference .	option	-
	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
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-
	Option **Description** *enable* Override WTP profile VAP settings. *disable* Use WTP profile VAP settings.		
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points .	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Automatically select tunnel VAPs. *disable* — Manually select VAPs.		
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	-
	Option / **Description** *enable* — Override WTP profile channel settings. *disable* — Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3

config radio-4

Parameter	Description	Type	Size
override-band	Enable to override the WTP profile band setting.	option	-
	Option / **Description** *enable* — Override the WTP profile band setting. *disable* — Use the WTP profile band setting.		
band	WiFi band that Radio 4 operates on.	option	-
	Option / **Description** *802.11a* — 802.11a. *802.11b* — 802.11b. *802.11g* — 802.11g/b. *802.11n* — 802.11n/g/b radio at 2.4GHz band. *802.11n-5G* — 802.11n/a at 5GHz. *802.11n,g-only* — 802.11n/g at 2.4GHz. *802.11g-only* — 802.11g. *802.11n-only* — 802.11n at 2.4GHz.		

Parameter	Description	Type	Size

Option	Description
802.11n-5G-only	802.11n at 5GHz.
802.11ac	802.11ac/n/a radio.
802.11ac,n-only	802.11ac/n.
802.11ac-only	802.11ac.
802.11ax-5G	802.11ax/ac/n/a at 5GHz.
802.11ax,ac-only	802.11ax/ac at 5GHz.
802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.
802.11ax-5G-only	802.11ax at 5GHz.
802.11ax	802.11ax/n/g/b at 2.4GHz.
802.11ax,n-only	802.11ax/n at 2.4GHz.
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.
802.11ax-only	802.11ax at 2.4GHz.

override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-

Option	Description
enable	Override the WTP profile spectrum analysis configuration.
disable	Use the WTP profile spectrum analysis configuration.

spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
enable	Enable spectrum analysis.
disable	Disable spectrum analysis.

override-txpower	Enable to override the WTP profile power level configuration.	option	-

Option	Description
enable	Override the WTP profile power level configuration.
disable	Use the WTP profile power level configuration.

Parameter	Description	Type	Size
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference . **Option** — **Description** *enable* — Enable automatic transmit power adjustment. *disable* — Disable automatic transmit power adjustment.	option	-
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
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
power-level	Radio power level as a percentage of the maximum transmit power .	integer	Minimum value: 0 Maximum value: 100
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings. **Option** — **Description** *enable* — Override WTP profile VAP settings. *disable* — Use WTP profile VAP settings.	option	-
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points . **Option** — **Description** *enable* — Automatically select tunnel VAPs. *disable* — Manually select VAPs.	option	-
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	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Override WTP profile channel settings. *disable* — Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3

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
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.

Parameter	Description	Type	Size

Option	Description
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.
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.

Parameter	Description	Type	Size
	Option / **Description** *224E* FAP224E. *231E* FAP231E. *S221E* FAPS221E. *S223E* FAPS223E. *321E* FAP321E. *431F* FAP431F. *432F* FAP432F. *433F* FAP433F. *231F* FAP231F. *234F* FAP234F. *23JF* FAP23JF. *U421E* FAPU421EV. *U422EV* FAPU422EV. *U423E* FAPU423EV. *U221EV* FAPU221EV. *U223EV* FAPU223EV. *U24JEV* FAPU24JEV. *U321EV* FAPU321EV. *U323EV* FAPU323EV. *U431F* FAPU431F. *U433F* FAPU433F.		
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
comment	Comment.	string	Maximum length: 63
uplink	Maximum uplink bandwidth for Virtual Access Points .	integer	Minimum value: 0 Maximum value: 2097152
downlink	Maximum downlink bandwidth for Virtual Access Points .	integer	Minimum value: 0 Maximum value: 2097152
uplink-sta	Maximum uplink bandwidth for clients .	integer	Minimum value: 0 Maximum value: 2097152
downlink-sta	Maximum downlink bandwidth for clients .	integer	Minimum value: 0 Maximum value: 2097152
burst	Enable/disable client rate burst.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* — Enable client rate burst. *disable* — Disable client rate burst.		
wmm	Enable/disable WiFi multi-media (WMM) control.	option	-
	Option / **Description** *enable* — Enable WiFi multi-media (WMM) control. *disable* — Disable WiFi multi-media (WMM) control.		
wmm-uapsd	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	option	-
	Option / **Description** *enable* — Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode. *disable* — Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.		
call-admission-control	Enable/disable WMM call admission control.	option	-
	Option / **Description** *enable* — Enable WMM call admission control. *disable* — Disable WMM call admission control.		
call-capacity	Maximum number of Voice over WLAN .	integer	Minimum value: 0 Maximum value: 60
bandwidth-admission-control	Enable/disable WMM bandwidth admission control.	option	-
	Option / **Description** *enable* — Enable WMM bandwidth admission control. *disable* — Disable WMM bandwidth admission control.		

Parameter	Description	Type	Size
bandwidth-capacity	Maximum bandwidth capacity allowed .	integer	Minimum value: 1 Maximum value: 600000
dscp-wmm-mapping	Enable/disable Differentiated Services Code Point (DSCP) mapping.	option	-

Option	Description
enable	Enable Differentiated Services Code Point (DSCP) mapping.
disable	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
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	-

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

Parameter	Description	Type	Size
wmm-vi-dscp	DSCP marking for video access .	integer	Minimum value: 0 Maximum value: 63
wmm-be-dscp	DSCP marking for best effort access .	integer	Minimum value: 0 Maximum value: 63
wmm-bk-dscp	DSCP marking for background access .	integer	Minimum value: 0 Maximum value: 63

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
comment	Comment.	var-string	Maximum length: 255
tunnel-type	Tunnel type.	option	-

Option	Description
l2tpv3	L2TPv3 Ethernet Pseudowire.
gre	GRE Ethernet tunnel.

wag-ip	IP Address of the wireless access gateway.	ipv4-address	Not Specified

Parameter	Description	Type	Size
wag-port	UDP port of the wireless access gateway.	integer	Minimum value: 0 Maximum value: 65535
ping-interval	Interval between two tunnel monitoring echo packets .	integer	Minimum value: 1 Maximum value: 65535
ping-number	Number of the tunnel monitoring echo packets .	integer	Minimum value: 1 Maximum value: 65535
return-packet-timeout	Window of time for the return packets from the tunnel's remote end .	integer	Minimum value: 1 Maximum value: 65535
dhcp-ip-addr	IP address of the monitoring DHCP request packet sent through the tunnel.	ipv4-address	Not Specified

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
comment	Comment.	string	Maximum length: 63
utm-log	Enable/disable UTM logging.	option	-

Parameter	Description	Type	Size
	Option / **Description** *enable* / Enable UTM logging. *disable* / 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	-
	Option / **Description** *disable* / Do not scan connections to botnet servers. *monitor* / Log connections to botnet servers. *block* / 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
mac	MAC address.	mac-address	Not Specified
policy	Allow or block the client with this MAC address.	option	-

Parameter	Description	Type	Size
	Option **Description** *allow* Allow the client with this MAC address. *deny* 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-policy	Allow or block the clients with MAC addresses that are not in the group.	option	-
	Option **Description** *allow* Allow the clients with MAC addresses that are not in the group. *deny* Block the clients with MAC addresses that are not in the group.		
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
engine-id	AC SNMP engineId 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
trap-high-mem-threshold	Memory usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100

config community

Parameter	Description	Type	Size
name	Community name.	string	Maximum length: 35
status	Enable/disable this SNMP community.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
query-v1-status	Enable/disable SNMP v1 queries.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
query-v2c-status	Enable/disable SNMP v2c queries.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
trap-v1-status	Enable/disable SNMP v1 traps.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

config hosts

Parameter	Description	Type	Size
ip	IPv4 address of the SNMP manager (host).	user	Not Specified

config user

Parameter	Description	Type	Size
status	SNMP User Enable	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
queries	Enable/disable SNMP queries for this user.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
trap-status	Enable/disable traps for this SNMP user.	option	-

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size
security-level	Security level for message authentication and encryption.	option	-

Option	Description
no-auth-no-priv	Message with no authentication and no privacy (encryption).
auth-no-priv	Message with authentication but no privacy (encryption).
auth-priv	Message with authentication and privacy (encryption).

Parameter	Description	Type	Size
auth-proto	Authentication protocol.	option	-

Option	Description
md5	HMAC-MD5-96 authentication protocol.
sha	HMAC-SHA-96 authentication protocol.

Parameter	Description	Type	Size
auth-pwd	Password for authentication protocol.	password	Not Specified
priv-proto	Privacy (encryption) protocol.	option	-

Option	Description
aes	CFB128-AES-128 symmetric encryption protocol.
des	CBC-DES symmetric encryption protocol.

Parameter	Description	Type	Size
	Option / **Description** *aes256* / CFB128-AES-256 symmetric encryption protocol. *aes256cisco* / CFB128-AES-256 symmetric encryption protocol compatible with CISCO.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified
notify-hosts	Configure SNMP User Notify Hosts.	ipv4-address	Not Specified

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
bssid	Access Point's (AP's) BSSID.	mac-address	Not Specified
ssid	Access Point's (AP's) SSID.	string	Maximum length: 32
status	Access Point's (AP's) status: rogue, accepted, or supressed.	option	-
	Option / **Description** *rogue* / Rogue AP. *accepted* / Accepted AP. *suppressed* / 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
[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
<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
<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
[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
<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
[wtp-id]	WTP ID.	string	Maximum length: -1

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.