



FortiOS - CLI Reference

Version 6.2.17

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



May 27, 2025

FortiOS 6.2.17 CLI Reference

01-6217-685877-20250527

TABLE OF CONTENTS

Change Log	15
FortiOS CLI reference	16
Availability of commands and options	16
Command tree	16
CLI configuration commands	18
alertemail	19
config alertemail setting	19
antivirus	26
config antivirus heuristic	26
config antivirus profile	26
config antivirus quarantine	50
config antivirus settings	55
application	57
config application custom	57
config application group	58
config application list	59
config application name	67
config application rule-settings	69
authentication	70
config authentication rule	70
config authentication scheme	72
config authentication setting	74
certificate	76
config certificate ca	76
config certificate crt	77
config certificate local	79
config certificate remote	82
cifs	83
config cifs domain-controller	83
config cifs profile	84
dlp	87
config dlp filepattern	87
config dlp fp-doc-source	90
config dlp sensitivity	93
config dlp sensor	94
config dlp settings	99
dnsfilter	101
config dnsfilter domain-filter	101
config dnsfilter profile	102
dpsdk	108
config dpsdk cpus	108
config dpsdk global	109
emailfilter	112
config emailfilter bwl	112

config emailfilter bword	114
config emailfilter dnsbl	116
config emailfilter fortishield	117
config emailfilter iptrust	118
config emailfilter mheader	119
config emailfilter options	121
config emailfilter profile	121
endpoint-control	131
config endpoint-control fctems	131
config endpoint-control settings	132
extender-controller	134
config extender-controller extender	134
firewall	140
config firewall DoS-policy	142
config firewall DoS-policy6	144
config firewall acl	147
config firewall acl6	148
config firewall address	149
config firewall address6	154
config firewall address6-template	157
config firewall addrgrp	159
config firewall addrgrp6	160
config firewall auth-portal	161
config firewall central-snat-map	162
config firewall consolidated policy	164
config firewall dnstranslation	174
config firewall identity-based-route	175
config firewall interface-policy	176
config firewall interface-policy6	179
config firewall internet-service	182
config firewall internet-service-addition	184
config firewall internet-service-append	186
config firewall internet-service-custom	186
config firewall internet-service-custom-group	188
config firewall internet-service-definition	188
config firewall internet-service-extension	190
config firewall internet-service-group	193
config firewall internet-service-ipbl-reason	194
config firewall internet-service-ipbl-vendor	194
config firewall internet-service-list	195
config firewall internet-service-owner	195
config firewall internet-service-reputation	196
config firewall internet-service-sld	196
config firewall ipmacbinding setting	197
config firewall ipmacbinding table	197
config firewall ippool	198
config firewall ippool6	200
config firewall ipv6-eh-filter	201
config firewall ip-translation	202

config firewall ldb-monitor	203
config firewall local-in-policy	205
config firewall local-in-policy6	206
config firewall multicast-address	207
config firewall multicast-address6	209
config firewall multicast-policy	210
config firewall multicast-policy6	212
config firewall policy	214
config firewall policy46	233
config firewall policy6	235
config firewall policy64	246
config firewall profile-group	249
config firewall profile-protocol-options	250
config firewall proxy-address	269
config firewall proxy-addgrp	273
config firewall proxy-policy	274
config firewall schedule group	281
config firewall schedule onetime	282
config firewall schedule recurring	282
config firewall security-policy	283
config firewall service category	290
config firewall service custom	290
config firewall service group	294
config firewall shaper per-ip-shaper	295
config firewall shaper traffic-shaper	296
config firewall shaping-policy	299
config firewall shaping-profile	303
config firewall sniffer	306
config firewall ssh host-key	311
config firewall ssh local-ca	312
config firewall ssh local-key	313
config firewall ssh setting	314
config firewall ssl setting	315
config firewall ssl-server	317
config firewall ssl-ssh-profile	320
config firewall traffic-class	335
config firewall ttl-policy	336
config firewall vip	337
config firewall vip46	366
config firewall vip6	369
config firewall vip64	397
config firewall vipgrp	400
config firewall vipgrp46	401
config firewall vipgrp6	402
config firewall vipgrp64	403
config firewall wildcard-fqdn custom	403
config firewall wildcard-fqdn group	404
ftp-proxy	406
config ftp-proxy explicit	406

icap	408
config icap profile	408
config icap server	411
ips	413
config ips custom	413
config ips decoder	415
config ips global	415
config ips rule	419
config ips rule-settings	422
config ips sensor	422
config ips settings	431
config ips view-map	432
log	434
config log custom-field	435
config log disk filter	435
config log disk setting	441
config log eventfilter	446
config log fortianalyzer filter	448
config log fortianalyzer override-filter	450
config log fortianalyzer override-setting	453
config log fortianalyzer setting	457
config log fortianalyzer2 filter	461
config log fortianalyzer2 override-filter	463
config log fortianalyzer2 override-setting	465
config log fortianalyzer2 setting	469
config log fortianalyzer3 filter	473
config log fortianalyzer3 override-filter	475
config log fortianalyzer3 override-setting	477
config log fortianalyzer3 setting	481
config log fortianalyzer-cloud filter	485
config log fortianalyzer-cloud override-filter	487
config log fortianalyzer-cloud override-setting	489
config log fortianalyzer-cloud setting	490
config log fortiguard filter	493
config log fortiguard override-filter	495
config log fortiguard override-setting	497
config log fortiguard setting	499
config log gui-display	501
config log memory filter	502
config log memory global-setting	507
config log memory setting	508
config log null-device filter	509
config log null-device setting	511
config log setting	511
config log syslogd filter	516
config log syslogd override-filter	518
config log syslogd override-setting	520
config log syslogd setting	524
config log syslogd2 filter	528

config log syslogd2 override-filter	530
config log syslogd2 override-setting	532
config log syslogd2 setting	536
config log syslogd3 filter	540
config log syslogd3 override-filter	542
config log syslogd3 override-setting	544
config log syslogd3 setting	548
config log syslogd4 filter	552
config log syslogd4 override-filter	554
config log syslogd4 override-setting	556
config log syslogd4 setting	560
config log threat-weight	564
config log webtrends filter	574
config log webtrends setting	576
monitoring	577
config monitoring np6-ipsec-engine	577
config monitoring npu-hpe	578
report	580
config report chart	580
config report dataset	590
config report layout	592
config report setting	602
config report style	604
config report theme	608
router	612
config router access-list	612
config router access-list6	614
config router aspath-list	615
config router auth-path	616
config router bfd	616
config router bfd6	617
config router bgp	617
config router community-list	656
config router isis	657
config router key-chain	670
config router multicast	671
config router multicast6	680
config router multicast-flow	682
config router ospf	683
config router ospf6	698
config router policy	711
config router policy6	714
config router prefix-list	715
config router prefix-list6	717
config router rip	718
config router ripng	725
config router route-map	731
config router setting	736
config router static	737

config router static6	740
ssh-filter	742
config ssh-filter profile	742
switch-controller	747
config switch-controller 802-1X-settings	748
config switch-controller auto-config custom	749
config switch-controller auto-config default	751
config switch-controller auto-config policy	752
config switch-controller custom-command	754
config switch-controller flow-tracking	755
config switch-controller global	758
config switch-controller igmp-snooping	762
config switch-controller lldp-profile	763
config switch-controller lldp-settings	767
config switch-controller location	768
config switch-controller managed-switch	773
config switch-controller network-monitor-settings	801
config switch-controller qos dot1p-map	802
config switch-controller qos ip-dscp-map	806
config switch-controller qos qos-policy	809
config switch-controller qos queue-policy	810
config switch-controller quarantine	813
config switch-controller remote-log	814
config switch-controller security-policy 802-1X	817
config switch-controller security-policy local-access	820
config switch-controller sflow	822
config switch-controller snmp-community	823
config switch-controller snmp-sysinfo	826
config switch-controller snmp-trap-threshold	827
config switch-controller snmp-user	829
config switch-controller storm-control	831
config switch-controller storm-control-policy	832
config switch-controller stp-instance	834
config switch-controller stp-settings	835
config switch-controller switch-group	837
config switch-controller switch-interface-tag	838
config switch-controller switch-log	839
config switch-controller switch-profile	840
config switch-controller system	842
config switch-controller traffic-policy	843
config switch-controller traffic-sniffer	845
config switch-controller virtual-port-pool	847
system	848
config system 3g-modem custom	851
config system accprofile	852
config system admin	862
config system affinity-interrupt	869
config system affinity-packet-redistribution	870
config system alarm	871

config system alias	874
config system api-user	875
config system arp-table	876
config system automation-action	877
config system automation-destination	882
config system automation-stitch	882
config system automation-trigger	883
config system autoupdate push-update	887
config system autoupdate schedule	887
config system autoupdate tunneling	888
config system auto-install	890
config system auto-script	891
config system bypass	892
config system central-management	894
config system cluster-sync	899
config system console	901
config system csf	903
config system custom-language	905
config system ddns	906
config system dedicated-mgmt	908
config system dhcp server	909
config system dhcp6 server	920
config system dnp3-proxy	924
config system dns	925
config system dns-database	927
config system dns-server	930
config system dscp-based-priority	931
config system elbc	932
config system email-server	933
config system external-resource	935
config system fips-cc	937
config system fm	937
config system fortiguard	939
config system fortimanager	945
config system fortisandbox	946
config system fsso-polling	947
config system ftm-push	948
config system geneve	949
config system geoip-override	950
config system global	951
config system gre-tunnel	988
config system ha	990
config system ha-monitor	1003
config system interface	1003
config system ipip-tunnel	1052
config system ipsec-aggregate	1053
config system ips-urlfilter-dns	1054
config system ips-urlfilter-dns6	1055
config system ipv6-neighbor-cache	1055

config system ipv6-tunnel	1056
config system isf-queue-profile	1057
config system link-monitor	1058
config system lldp network-policy	1061
config system lte-modem	1069
config system mac-address-table	1073
config system management-tunnel	1074
config system mobile-tunnel	1075
config system modem	1078
config system nat64	1085
config system nd-proxy	1086
config system netflow	1087
config system network-visibility	1088
config system np6	1090
config system np6xlite	1103
config system npu	1115
config system ntp	1127
config system object-tagging	1130
config system password-policy	1132
config system password-policy-guest-admin	1134
config system physical-switch	1136
config system pppoe-interface	1137
config system probe-response	1139
config system proxy-arp	1140
config system ptp	1141
config system replacemsg admin	1142
config system replacemsg alertmail	1143
config system replacemsg auth	1144
config system replacemsg device-detection-portal	1145
config system replacemsg fortiguard-wf	1145
config system replacemsg ftp	1146
config system replacemsg http	1147
config system replacemsg icap	1148
config system replacemsg mail	1149
config system replacemsg nac-quar	1150
config system replacemsg nntp	1151
config system replacemsg spam	1151
config system replacemsg sslvpn	1152
config system replacemsg traffic-quota	1153
config system replacemsg utm	1154
config system replacemsg webproxy	1155
config system replacemsg-group	1156
config system replacemsg-image	1169
config system resource-limits	1169
config system saml	1172
config system sdn-connector	1175
config system session-helper	1181
config system session-ttl	1183
config system settings	1184

config system sflow	1203
config system sit-tunnel	1204
config system smc-ntp	1205
config system sms-server	1206
config system snmp community	1207
config system snmp sysinfo	1213
config system snmp user	1214
config system speed-test-server	1218
config system sso-admin	1219
config system storage	1220
config system stp	1222
config system switch-interface	1223
config system tos-based-priority	1225
config system vdom	1226
config system vdom-dns	1227
config system vdom-exception	1228
config system vdom-link	1230
config system vdom-netflow	1231
config system vdom-property	1231
config system vdom-radius-server	1233
config system vdom-sflow	1234
config system virtual-switch	1235
config system virtual-wan-link	1237
config system virtual-wire-pair	1253
config system vxlan	1254
config system wccp	1256
config system wireless ap-status	1259
config system wireless settings	1261
config system zone	1264
user	1266
config user adgrp	1266
config user domain-controller	1267
config user exchange	1268
config user fortitoken	1270
config user fsso	1271
config user fsso-polling	1275
config user group	1277
config user krb-keytab	1282
config user ldap	1283
config user local	1287
config user password-policy	1291
config user peer	1291
config user peergrp	1293
config user pop3	1294
config user quarantine	1295
config user radius	1296
config user saml	1306
config user security-exempt-list	1307
config user setting	1308

config user tacacs+	1312
voip	1315
config voip profile	1315
vpn	1335
config vpn certificate ca	1335
config vpn certificate crt	1337
config vpn certificate local	1338
config vpn certificate ocsdp-server	1341
config vpn certificate remote	1342
config vpn certificate setting	1343
config vpn ipsec concentrator	1347
config vpn ipsec forticlient	1347
config vpn ipsec manualkey	1348
config vpn ipsec manualkey-interface	1350
config vpn ipsec phase1	1352
config vpn ipsec phase1-interface	1371
config vpn ipsec phase2	1395
config vpn ipsec phase2-interface	1403
config vpn l2tp	1411
config vpn ocvpn	1412
config vpn pptp	1415
config vpn ssl settings	1416
config vpn ssl web host-check-software	1428
config vpn ssl web portal	1429
config vpn ssl web realm	1445
config vpn ssl web user-bookmark	1445
config vpn ssl web user-group-bookmark	1450
waf	1454
config waf main-class	1454
config waf profile	1454
config waf signature	1479
config waf sub-class	1479
wanopt	1481
config wanopt auth-group	1481
config wanopt cache-service	1483
config wanopt content-delivery-network-rule	1486
config wanopt peer	1492
config wanopt profile	1493
config wanopt remote-storage	1503
config wanopt settings	1504
config wanopt webcache	1506
web-proxy	1510
config web-proxy debug-url	1510
config web-proxy explicit	1511
config web-proxy forward-server	1516
config web-proxy forward-server-group	1517
config web-proxy global	1518
config web-proxy profile	1521
config web-proxy url-match	1525

config web-proxy wisp	1526
webfilter	1528
config webfilter content	1528
config webfilter content-header	1530
config webfilter fortiguard	1531
config webfilter ftgd-local-cat	1533
config webfilter ftgd-local-rating	1534
config webfilter ips-urlfilter-cache-setting	1535
config webfilter ips-urlfilter-setting	1535
config webfilter ips-urlfilter-setting6	1536
config webfilter override	1536
config webfilter profile	1538
config webfilter search-engine	1554
config webfilter urlfilter	1555
wireless-controller	1558
config wireless-controller address	1559
config wireless-controller addrgrp	1559
config wireless-controller ap-status	1560
config wireless-controller ble-profile	1561
config wireless-controller bonjour-profile	1563
config wireless-controller global	1564
config wireless-controller hotspot20 anqp-3gpp-cellular	1567
config wireless-controller hotspot20 anqp-ip-address-type	1568
config wireless-controller hotspot20 anqp-nai-realm	1569
config wireless-controller hotspot20 anqp-network-auth-type	1572
config wireless-controller hotspot20 anqp-roaming-consortium	1573
config wireless-controller hotspot20 anqp-venue-name	1574
config wireless-controller hotspot20 h2qp-conn-capability	1575
config wireless-controller hotspot20 h2qp-operator-name	1577
config wireless-controller hotspot20 h2qp-osu-provider	1578
config wireless-controller hotspot20 h2qp-wan-metric	1580
config wireless-controller hotspot20 hs-profile	1581
config wireless-controller hotspot20 icon	1588
config wireless-controller hotspot20 qos-map	1590
config wireless-controller inter-controller	1591
config wireless-controller log	1593
config wireless-controller qos-profile	1597
config wireless-controller region	1601
config wireless-controller setting	1602
config wireless-controller snmp	1608
config wireless-controller timers	1612
config wireless-controller utm-profile	1614
config wireless-controller vap	1615
config wireless-controller vap-group	1639
config wireless-controller wag-profile	1640
config wireless-controller wids-profile	1641
config wireless-controller wtp	1649
config wireless-controller wtp-group	1669
config wireless-controller wtp-profile	1672

Included devices 1726

Change Log

Date	Change Description
2025-05-27	Initial release of the FortiOS 6.2.17 CLI Reference.

FortiOS CLI reference

This document describes FortiOS 6.2.17 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI). For information on using the CLI, see the [FortiOS 6.2.17 Administration Guide](#), which contains information such as:

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

Availability of commands and options

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

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

FortiGate model

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

Hardware configuration

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

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

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

Command tree

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

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

CLI configuration commands

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

alertemail

This section includes syntax for the following commands:

- [config alertemail setting on page 19](#)

config alertemail setting

Configure alert email settings.

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

config alertemail setting

Parameter	Description	Type	Size						
FDS-license-expiring-days	Number of days to send alert email prior to FortiGuard license expiration (1 - 100 days, default = 100).	integer	Minimum value: 1 Maximum value: 100						
FDS-license-expiring-warning	Enable/disable FortiGuard license expiration warnings in alert email.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard license expiration warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard license expiration warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.	<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.		
Option	Description								
<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.								
<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.								
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard update logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard update logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard update logs in alert email.	<i>disable</i>	Disable FortiGuard update logs in alert email.		
Option	Description								
<i>enable</i>	Enable FortiGuard update logs in alert email.								
<i>disable</i>	Disable FortiGuard update logs in alert email.								
FIPS-CC-errors	Enable/disable FIPS and Common Criteria error logs in alert email.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FIPS and Common Criteria error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FIPS and Common Criteria error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.	<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.		
Option	Description								
<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.								
<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.								
FSSO-disconnect-logs	Enable/disable logging of FSSO collector agent disconnect.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging of FSSO collector agent disconnect.</td></tr><tr><td><i>disable</i></td><td>Disable logging of FSSO collector agent disconnect.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of FSSO collector agent disconnect.	<i>disable</i>	Disable logging of FSSO collector agent disconnect.		
Option	Description								
<i>enable</i>	Enable logging of FSSO collector agent disconnect.								
<i>disable</i>	Disable logging of FSSO collector agent disconnect.								
HA-logs	Enable/disable HA logs in alert email.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable HA logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable HA logs in alert email.	<i>disable</i>	Disable HA logs in alert email.		
Option	Description								
<i>enable</i>	Enable HA logs in alert email.								
<i>disable</i>	Disable HA logs in alert email.								
IPS-logs	Enable/disable IPS logs in alert email.	option	-						

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

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

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable firewall authentication failure logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable firewall authentication failure logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable firewall authentication failure logs in alert email.	<i>disable</i>	Disable firewall authentication failure logs in alert email.		
	Option	Description							
	<i>enable</i>	Enable firewall authentication failure logs in alert email.							
<i>disable</i>	Disable firewall authentication failure logs in alert email.								
fortiguard-log-quota-warning	Enable/disable FortiCloud log quota warnings in alert email.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud log quota warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud log quota warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.	<i>disable</i>	Disable FortiCloud log quota warnings in alert email.		
	Option	Description							
	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.							
<i>disable</i>	Disable FortiCloud log quota warnings in alert email.								
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999						
local-disk-usage	Disk usage percentage at which to send alert email (1 - 99 percent, default = 75).	integer	Minimum value: 1 Maximum value: 99						
log-disk-usage-warning	Enable/disable disk usage warnings in alert email.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable disk usage warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable disk usage warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable disk usage warnings in alert email.	<i>disable</i>	Disable disk usage warnings in alert email.		
	Option	Description							
	<i>enable</i>	Enable disk usage warnings in alert email.							
<i>disable</i>	Disable disk usage warnings in alert email.								
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						
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999						
severity	Lowest severity level to log.	option	-						

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.		
	Option	Description																			
	<i>emergency</i>	Emergency level.																			
	<i>alert</i>	Alert level.																			
	<i>critical</i>	Critical level.																			
	<i>error</i>	Error level.																			
	<i>warning</i>	Warning level.																			
	<i>notification</i>	Notification level.																			
	<i>information</i>	Information level.																			
<i>debug</i>	Debug level.																				
ssh-logs	Enable/disable SSH logs in alert email.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable SSH logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH logs in alert email.	<i>disable</i>	Disable SSH logs in alert email.														
	Option	Description																			
	<i>enable</i>	Enable SSH logs in alert email.																			
<i>disable</i>	Disable SSH logs in alert email.																				
sslvpn-authentication-errors-logs	Enable/disable SSL-VPN authentication error logs in alert email.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN authentication error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN authentication error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.	<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.														
	Option	Description																			
	<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.																			
<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.																				
username	Name that appears in the From: field of alert emails (max. 36 characters).	string	Maximum length: 63																		
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable violation traffic logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable violation traffic logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable violation traffic logs in alert email.	<i>disable</i>	Disable violation traffic logs in alert email.														
	Option	Description																			
	<i>enable</i>	Enable violation traffic logs in alert email.																			
<i>disable</i>	Disable violation traffic logs in alert email.																				
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999																		
webfilter-logs	Enable/disable web filter logs in alert email.	option	-																		

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable web filter logs in alert email.	
	<i>disable</i>	Disable web filter logs in alert email.	

antivirus

This section includes syntax for the following commands:

- [config antivirus heuristic on page 26](#)
- [config antivirus profile on page 26](#)
- [config antivirus quarantine on page 50](#)
- [config antivirus settings on page 55](#)

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

config antivirus profile

Configure AntiVirus profiles.

```
config antivirus profile
  Description: Configure AntiVirus profiles.
  edit <name>
    set analytics-bl-filetype {integer}
    set analytics-db [disable|enable]
```

```

set analytics-max-upload {integer}
set analytics-wl-filetype {integer}
set av-block-log [enable|disable]
set av-virus-log [enable|disable]
config cifs
    Description: Configure CIFS AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set options {option1}, {option2}, ...
    set outbreak-prevention [disabled|files|...]
end
set comment {var-string}
config content-disarm
    Description: AV Content Disarm and Reconstruction settings.
    set cover-page [disable|enable]
    set detect-only [disable|enable]
    set office-action [disable|enable]
    set office-dde [disable|enable]
    set office-embed [disable|enable]
    set office-hylink [disable|enable]
    set office-linked [disable|enable]
    set office-macro [disable|enable]
    set original-file-destination [fortisandbox|quarantine|...]
    set pdf-act-form [disable|enable]
    set pdf-act-gotor [disable|enable]
    set pdf-act-java [disable|enable]
    set pdf-act-launch [disable|enable]
    set pdf-act-movie [disable|enable]
    set pdf-act-sound [disable|enable]
    set pdf-embedfile [disable|enable]
    set pdf-hyperlink [disable|enable]
    set pdf-javacode [disable|enable]
end
set extended-log [enable|disable]
set ftgd-analytics [disable|suspicious|...]
config ftp
    Description: Configure FTP AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set options {option1}, {option2}, ...
    set outbreak-prevention [disabled|files|...]
end
config http
    Description: Configure HTTP AntiVirus options.
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set content-disarm [disable|enable]
    set emulator [enable|disable]
    set options {option1}, {option2}, ...
    set outbreak-prevention [disabled|files|...]
end
config imap
    Description: Configure IMAP AntiVirus options.
    set archive-block {option1}, {option2}, ...

```

```

        set archive-log {option1}, {option2}, ...
        set content-disarm [disable|enable]
        set emulator [enable|disable]
        set executables [default|virus]
        set options {option1}, {option2}, ...
        set outbreak-prevention [disabled|files|...]
    end
    config mapi
        Description: Configure MAPI AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set executables [default|virus]
        set options {option1}, {option2}, ...
        set outbreak-prevention [disabled|files|...]
    end
    set mobile-malware-db [disable|enable]
    config nac-quar
        Description: Configure AntiVirus quarantine settings.
        set expiry {user}
        set infected [none|quar-src-ip]
        set log [enable|disable]
    end
    config nntp
        Description: Configure NNTP AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set options {option1}, {option2}, ...
        set outbreak-prevention [disabled|files|...]
    end
    config outbreak-prevention
        Description: Configure Virus Outbreak Prevention settings.
        set external-blocklist [disable|enable]
        set ftgd-service [disable|enable]
    end
    config pop3
        Description: Configure POP3 AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set content-disarm [disable|enable]
        set emulator [enable|disable]
        set executables [default|virus]
        set options {option1}, {option2}, ...
        set outbreak-prevention [disabled|files|...]
    end
    set replacemsg-group {string}
    set scan-mode [default|legacy]
    config smtp
        Description: Configure SMTP AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set content-disarm [disable|enable]
        set emulator [enable|disable]
        set executables [default|virus]
        set options {option1}, {option2}, ...

```

```

        set outbreak-prevention [disabled|files|...]
    end
    config ssh
        Description: Configure SFTP and SCP AntiVirus options.
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set options {option1}, {option2}, ...
        set outbreak-prevention [disabled|files|...]
    end
next
end

```

config antivirus profile

Parameter	Description	Type	Size						
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Use only the standard AV signature databases.</td></tr><tr><td>enable</td><td>Also use the FortiSandbox signature database.</td></tr></table>			Option	Description	disable	Use only the standard AV signature databases.	enable	Also use the FortiSandbox signature database.
Option	Description								
disable	Use only the standard AV signature databases.								
enable	Also use the FortiSandbox signature database.								
analytics-max-upload	Maximum size of files that can be uploaded to FortiSandbox (1 - 395 MBytes, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **						
analytics-wl-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295						
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>			Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
av-virus-log	Enable/disable AntiVirus logging.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
comment	Comment.	var-string	Maximum length: 255
extended-log	Enable/disable extended logging for antivirus.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-
	Option	Description	
	<i>disable</i>	Do not upload files to FortiSandbox.	
	<i>suspicious</i>	Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.	
	<i>everything</i>	Submit all files scanned by AntiVirus to FortiSandbox. AntiVirus may not scan all files.	
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-
	Option	Description	
	<i>disable</i>	Do not use the mobile malware signature database.	
	<i>enable</i>	Also use the mobile malware signature database.	
name	Profile name.	string	Maximum length: 35
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35
scan-mode	Choose between default scan mode and legacy scan mode.	option	-
	Option	Description	
	<i>default</i>	Aggregate scanning mode.	
	<i>legacy</i>	Force scanunit to scan all files.	

** Values may differ between models.

config cifs

Parameter	Description	Type	Size																				
archive-block	Select the archive types to block.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>fileslimit</i></td><td>Block exceeded archive files limit.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives.	<i>mailbomb</i>	Block mail bomb archives.	<i>fileslimit</i>	Block exceeded archive files limit.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.		
Option	Description																						
<i>encrypted</i>	Block encrypted archives.																						
<i>corrupted</i>	Block corrupted archives.																						
<i>partiallycorrupted</i>	Block partially corrupted archives.																						
<i>multipart</i>	Block multipart archives.																						
<i>nested</i>	Block nested archives.																						
<i>mailbomb</i>	Block mail bomb archives.																						
<i>fileslimit</i>	Block exceeded archive files limit.																						
<i>timeout</i>	Block scan timeout.																						
<i>unhandled</i>	Block archives that FortiOS cannot open.																						
archive-log	Select the archive types to log.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>fileslimit</i></td><td>Log exceeded archive files limit.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.		
Option	Description																						
<i>encrypted</i>	Log encrypted archives.																						
<i>corrupted</i>	Log corrupted archives.																						
<i>partiallycorrupted</i>	Log partially corrupted archives.																						
<i>multipart</i>	Log multipart archives.																						
<i>nested</i>	Log nested archives.																						
<i>mailbomb</i>	Log mail bomb archives.																						
<i>fileslimit</i>	Log exceeded archive files limit.																						
<i>timeout</i>	Log scan timeout.																						
<i>unhandled</i>	Log archives that FortiOS cannot open.																						
emulator	Enable/disable the virus emulator.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																
Option	Description																						
<i>enable</i>	Enable the virus emulator.																						
<i>disable</i>	Disable the virus emulator.																						
options	Enable/disable CIFS AntiVirus scanning, monitoring, and quarantine.	option	-																				

Parameter	Description	Type	Size
	Option	Description	
	<i>scan</i>	Enable CIFS antivirus scanning.	
	<i>avmonitor</i>	Enable CIFS antivirus logging.	
	<i>quarantine</i>	Enable CIFS antivirus quarantine. Files are quarantined depending on quarantine settings.	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option	Description	
	<i>disabled</i>	Disabled.	
	<i>files</i>	Analyze files as sent, not the content of archives.	
	<i>full-archive</i>	Analyze files including the content of archives.	

config content-disarm

Parameter	Description	Type	Size
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-
	Option	Description	
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.	
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-
	Option	Description	
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.	
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-
	Option	Description	
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.	

Parameter	Description	Type	Size						
office-dde	Enable/disable stripping of Dynamic Data Exchange events in Microsoft Office documents.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
original-file-destination	Destination to send original file if active content is removed.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortisandbox</i></td><td>Send original file to configured FortiSandbox.</td></tr></table>	Option	Description	<i>fortisandbox</i>	Send original file to configured FortiSandbox.				
Option	Description								
<i>fortisandbox</i>	Send original file to configured FortiSandbox.								

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>quarantine</i></td><td>Send original file to quarantine.</td></tr><tr><td><i>discard</i></td><td>Original file will be discarded after content disarm.</td></tr></table>	Option	Description	<i>quarantine</i>	Send original file to quarantine.	<i>discard</i>	Original file will be discarded after content disarm.		
Option	Description								
<i>quarantine</i>	Send original file to quarantine.								
<i>discard</i>	Original file will be discarded after content disarm.								
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
Option	Description								
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.								
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.								
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-						

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

config ftp

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

Parameter	Description	Type	Size
	Option	Description	
	<i>fileslimit</i>	Block exceeded archive files limit.	
	<i>timeout</i>	Block scan timeout.	
	<i>unhandled</i>	Block archives that FortiOS cannot open.	
archive-log	Select the archive types to log.	option	-
	Option	Description	
	<i>encrypted</i>	Log encrypted archives.	
	<i>corrupted</i>	Log corrupted archives.	
	<i>partiallycorrupted</i>	Log partially corrupted archives.	
	<i>multipart</i>	Log multipart archives.	
	<i>nested</i>	Log nested archives.	
	<i>mailbomb</i>	Log mail bomb archives.	
	<i>fileslimit</i>	Log exceeded archive files limit.	
	<i>timeout</i>	Log scan timeout.	
	<i>unhandled</i>	Log archives that FortiOS cannot open.	
emulator	Enable/disable the virus emulator.	option	-
	Option	Description	
	<i>enable</i>	Enable the virus emulator.	
	<i>disable</i>	Disable the virus emulator.	
options	Enable/disable FTP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option	Description	
	<i>scan</i>	Enable FTP antivirus scanning.	
	<i>avmonitor</i>	Enable FTP antivirus logging.	
	<i>quarantine</i>	Enable FTP antivirus quarantine. Files are quarantined depending on quarantine settings.	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disabled</i>	Disabled.	
	<i>files</i>	Analyze files as sent, not the content of archives.	
	<i>full-archive</i>	Analyze files including the content of archives.	

config http

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

Parameter	Description	Type	Size								
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction for this protocol.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction for this protocol.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.				
Option	Description										
<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.										
<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.										
emulator	Enable/disable the virus emulator.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.				
Option	Description										
<i>enable</i>	Enable the virus emulator.										
<i>disable</i>	Disable the virus emulator.										
options	Enable/disable HTTP AntiVirus scanning, monitoring, and quarantine.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>scan</i></td><td>Enable HTTP antivirus scanning.</td></tr><tr><td><i>avmonitor</i></td><td>Enable HTTP antivirus logging.</td></tr><tr><td><i>quarantine</i></td><td>Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.</td></tr></table>	Option	Description	<i>scan</i>	Enable HTTP antivirus scanning.	<i>avmonitor</i>	Enable HTTP antivirus logging.	<i>quarantine</i>	Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.		
Option	Description										
<i>scan</i>	Enable HTTP antivirus scanning.										
<i>avmonitor</i>	Enable HTTP antivirus logging.										
<i>quarantine</i>	Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.										
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Disabled.</td></tr><tr><td><i>files</i></td><td>Analyze files as sent, not the content of archives.</td></tr><tr><td><i>full-archive</i></td><td>Analyze files including the content of archives.</td></tr></table>	Option	Description	<i>disabled</i>	Disabled.	<i>files</i>	Analyze files as sent, not the content of archives.	<i>full-archive</i>	Analyze files including the content of archives.		
Option	Description										
<i>disabled</i>	Disabled.										
<i>files</i>	Analyze files as sent, not the content of archives.										
<i>full-archive</i>	Analyze files including the content of archives.										

config imap

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

Parameter	Description	Type	Size
	Option	Description	
	<i>partiallycorrupted</i>	Block partially corrupted archives.	
	<i>multipart</i>	Block multipart archives.	
	<i>nested</i>	Block nested archives.	
	<i>mailbomb</i>	Block mail bomb archives.	
	<i>fileslimit</i>	Block exceeded archive files limit.	
	<i>timeout</i>	Block scan timeout.	
	<i>unhandled</i>	Block archives that FortiOS cannot open.	
	archive-log	Select the archive types to log.	option
	Option	Description	
	<i>encrypted</i>	Log encrypted archives.	
	<i>corrupted</i>	Log corrupted archives.	
	<i>partiallycorrupted</i>	Log partially corrupted archives.	
	<i>multipart</i>	Log multipart archives.	
	<i>nested</i>	Log nested archives.	
	<i>mailbomb</i>	Log mail bomb archives.	
	<i>fileslimit</i>	Log exceeded archive files limit.	
	<i>timeout</i>	Log scan timeout.	
	<i>unhandled</i>	Log archives that FortiOS cannot open.	
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-
	Option	Description	
	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	
	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.	
emulator	Enable/disable the virus emulator.	option	-
	Option	Description	
	<i>enable</i>	Enable the virus emulator.	
	<i>disable</i>	Disable the virus emulator.	

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

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

options	Enable/disable IMAP AntiVirus scanning, monitoring, and quarantine.	option	-

Option	Description
<i>scan</i>	Enable IMAP antivirus scanning.
<i>avmonitor</i>	Enable IMAP antivirus logging.
<i>quarantine</i>	Enable IMAP antivirus quarantine. Files are quarantined depending on quarantine settings.

outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-

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

config mapi

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

Option	Description
<i>encrypted</i>	Block encrypted archives.
<i>corrupted</i>	Block corrupted archives.
<i>partiallycorrupted</i>	Block partially corrupted archives.
<i>multipart</i>	Block multipart archives.
<i>nested</i>	Block nested archives.
<i>mailbomb</i>	Block mail bomb archives.
<i>fileslimit</i>	Block exceeded archive files limit.

Parameter	Description	Type	Size
	Option	Description	
	<i>timeout</i>	Block scan timeout.	
	<i>unhandled</i>	Block archives that FortiOS cannot open.	
archive-log	Select the archive types to log.	option	-
	Option	Description	
	<i>encrypted</i>	Log encrypted archives.	
	<i>corrupted</i>	Log corrupted archives.	
	<i>partiallycorrupted</i>	Log partially corrupted archives.	
	<i>multipart</i>	Log multipart archives.	
	<i>nested</i>	Log nested archives.	
	<i>mailbomb</i>	Log mail bomb archives.	
	<i>fileslimit</i>	Log exceeded archive files limit.	
	<i>timeout</i>	Log scan timeout.	
	<i>unhandled</i>	Log archives that FortiOS cannot open.	
emulator	Enable/disable the virus emulator.	option	-
	Option	Description	
	<i>enable</i>	Enable the virus emulator.	
	<i>disable</i>	Disable the virus emulator.	
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-
	Option	Description	
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	
	<i>virus</i>	Treat Windows executables as viruses.	
options	Enable/disable MAPI AntiVirus scanning, monitoring, and quarantine.	option	-
	Option	Description	
	<i>scan</i>	Enable MAPI antivirus scanning.	
	<i>avmonitor</i>	Enable MAPI antivirus logging.	

Parameter	Description	Type	Size
	Option	Description	
	<i>quarantine</i>	Enable MAPI antivirus quarantine. Files are quarantined depending on quarantine settings.	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option	Description	
	<i>disabled</i>	Disabled.	
	<i>files</i>	Analyze files as sent, not the content of archives.	
	<i>full-archive</i>	Analyze files including the content of archives.	

config nac-quar

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

config nntp

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

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

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

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

config outbreak-prevention

Parameter	Description	Type	Size
external-blocklist	Enable/disable external malware blocklist.	option	-

Option	Description
<i>disable</i>	Disable external malware blocklist.
<i>enable</i>	Enable external malware blocklist.

ftgd-service	Enable/disable FortiGuard Virus outbreak prevention service.	option	-

Option	Description
<i>disable</i>	Disable FortiGuard Virus Outbreak Prevention service.
<i>enable</i>	Enable FortiGuard Virus Outbreak Prevention service.

config pop3

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

Option	Description
<i>encrypted</i>	Block encrypted archives.
<i>corrupted</i>	Block corrupted archives.
<i>partiallycorrupted</i>	Block partially corrupted archives.
<i>multipart</i>	Block multipart archives.
<i>nested</i>	Block nested archives.

Parameter	Description	Type	Size
	Option	Description	
	<i>mailbomb</i>	Block mail bomb archives.	
	<i>fileslimit</i>	Block exceeded archive files limit.	
	<i>timeout</i>	Block scan timeout.	
	<i>unhandled</i>	Block archives that FortiOS cannot open.	
archive-log	Select the archive types to log.	option	-
	Option	Description	
	<i>encrypted</i>	Log encrypted archives.	
	<i>corrupted</i>	Log corrupted archives.	
	<i>partiallycorrupted</i>	Log partially corrupted archives.	
	<i>multipart</i>	Log multipart archives.	
	<i>nested</i>	Log nested archives.	
	<i>mailbomb</i>	Log mail bomb archives.	
	<i>fileslimit</i>	Log exceeded archive files limit.	
	<i>timeout</i>	Log scan timeout.	
	<i>unhandled</i>	Log archives that FortiOS cannot open.	
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-
	Option	Description	
	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	
	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.	
emulator	Enable/disable the virus emulator.	option	-
	Option	Description	
	<i>enable</i>	Enable the virus emulator.	
	<i>disable</i>	Disable the virus emulator.	
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	
	<i>virus</i>	Treat Windows executables as viruses.	
options	Enable/disable POP3 AntiVirus scanning, monitoring, and quarantine.	option	-
	Option	Description	
	<i>scan</i>	Enable POP3 antivirus scanning.	
	<i>avmonitor</i>	Enable POP3 antivirus logging.	
	<i>quarantine</i>	Enable POP3 antivirus quarantine. Files are quarantined depending on quarantine settings.	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option	Description	
	<i>disabled</i>	Disabled.	
	<i>files</i>	Analyze files as sent, not the content of archives.	
	<i>full-archive</i>	Analyze files including the content of archives.	

config smtp

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

Parameter	Description	Type	Size																				
archive-log	Select the archive types to log.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>fileslimit</i></td><td>Log exceeded archive files limit.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives.	<i>mailbomb</i>	Log mail bomb archives.	<i>fileslimit</i>	Log exceeded archive files limit.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.		
Option	Description																						
<i>encrypted</i>	Log encrypted archives.																						
<i>corrupted</i>	Log corrupted archives.																						
<i>partiallycorrupted</i>	Log partially corrupted archives.																						
<i>multipart</i>	Log multipart archives.																						
<i>nested</i>	Log nested archives.																						
<i>mailbomb</i>	Log mail bomb archives.																						
<i>fileslimit</i>	Log exceeded archive files limit.																						
<i>timeout</i>	Log scan timeout.																						
<i>unhandled</i>	Log archives that FortiOS cannot open.																						
content-disarm	Enable Content Disarm and Reconstruction for this protocol.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction for this protocol.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction for this protocol.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.	<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.																
Option	Description																						
<i>disable</i>	Disable Content Disarm and Reconstruction for this protocol.																						
<i>enable</i>	Enable Content Disarm and Reconstruction for this protocol.																						
emulator	Enable/disable the virus emulator.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.																
Option	Description																						
<i>enable</i>	Enable the virus emulator.																						
<i>disable</i>	Disable the virus emulator.																						
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.																
Option	Description																						
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																						
<i>virus</i>	Treat Windows executables as viruses.																						
options	Enable/disable SMTP AntiVirus scanning, monitoring, and quarantine.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>scan</i></td><td>Enable SMTP antivirus scanning.</td></tr></table>	Option	Description	<i>scan</i>	Enable SMTP antivirus scanning.																		
Option	Description																						
<i>scan</i>	Enable SMTP antivirus scanning.																						

Parameter	Description	Type	Size
	Option	Description	
	<i>avmonitor</i>	Enable SMTP antivirus logging.	
	<i>quarantine</i>	Enable SMTP antivirus quarantine. Files are quarantined depending on quarantine settings.	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option	Description	
	<i>disabled</i>	Disabled.	
	<i>files</i>	Analyze files as sent, not the content of archives.	
	<i>full-archive</i>	Analyze files including the content of archives.	

config ssh

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

Parameter	Description	Type	Size
	Option	Description	
	<i>multipart</i>	Log multipart archives.	
	<i>nested</i>	Log nested archives.	
	<i>mailbomb</i>	Log mail bomb archives.	
	<i>fileslimit</i>	Log exceeded archive files limit.	
	<i>timeout</i>	Log scan timeout.	
	<i>unhandled</i>	Log archives that FortiOS cannot open.	
emulator	Enable/disable the virus emulator.	option	-
	Option	Description	
	<i>enable</i>	Enable the virus emulator.	
	<i>disable</i>	Disable the virus emulator.	
options	Enable/disable SFTP and SCP AntiVirus scanning, monitoring, and quarantine.	option	-
	Option	Description	
	<i>scan</i>	Enable SSH antivirus scanning.	
	<i>avmonitor</i>	Enable SSH antivirus logging.	
	<i>quarantine</i>	Enable SSH antivirus quarantine. Files are quarantined depending on quarantine settings.	
outbreak-prevention	Enable Virus Outbreak Prevention service.	option	-
	Option	Description	
	<i>disabled</i>	Disabled.	
	<i>files</i>	Analyze files as sent, not the content of archives.	
	<i>full-archive</i>	Analyze files including the content of archives.	

config antivirus quarantine



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGateRugged 30D, FortiGateRugged 35D.

Configure quarantine options.

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

config antivirus quarantine

Parameter	Description	Type	Size
agelimit	Age limit for quarantined files (0 - 479 hours, 0 means forever).	integer	Minimum value: 0 Maximum value: 479
destination	Choose whether to quarantine files to the FortiGate disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-

Option	Description
<i>NULL</i>	Files that would be quarantined are deleted.
<i>disk</i>	Quarantine files to the FortiGate hard disk.
<i>FortiAnalyzer</i>	FortiAnalyzer

drop-blocked	Do not quarantine dropped files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-

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

Parameter	Description	Type	Size

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

drop-infected	Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>nnntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>https</i>	HTTPS.
<i>ftps</i>	FTPS.

Parameter	Description	Type	Size

Option	Description
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

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

Option	Description
<i>drop-new</i>	Drop (delete) the most recently quarantined files.
<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.

maxfilesize	Maximum file size to quarantine (0 - 500 Mbytes, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 500
quarantine-quota	The amount of disk space to reserve for quarantining files (0 - 4294967295 Mbytes, depends on disk space).	integer	Minimum value: 0 Maximum value: 4294967295
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>ftps</i>	FTPS.

Parameter	Description	Type	Size

Option	Description
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

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

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

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

Option	Description
<i>imap</i>	IMAP.
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>http</i>	HTTP.
<i>ftp</i>	FTP.

Parameter	Description	Type	Size

Option	Description
<i>nntp</i>	NNTP.
<i>imaps</i>	IMAPS.
<i>smtps</i>	SMTPS.
<i>pop3s</i>	POP3S.
<i>https</i>	HTTPS.
<i>ftps</i>	FTPS.
<i>mapi</i>	MAPI.
<i>cifs</i>	CIFS.
<i>ssh</i>	SSH.

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
<i>normal</i>	Use the normal AntiVirus database.
<i>extended</i>	Use the extended AntiVirus database.
<i>extreme</i>	Use all available AntiVirus databases

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

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable grayware detection.	
	<i>disable</i>	Disable grayware detection.	
override-timeout	Override the large file scan timeout value in seconds (30 - 3600). Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600

application

This section includes syntax for the following commands:

- [config application custom on page 57](#)
- [config application group on page 58](#)
- [config application list on page 59](#)
- [config application name on page 67](#)
- [config application rule-settings on page 69](#)

config application custom

Configure custom application signatures.

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

config application custom

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

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

config application group

Configure firewall application groups.

```

config application group
    Description: Configure firewall application groups.
    edit <name>
        set application <id1>, <id2>, ...
        set category <id1>, <id2>, ...
        set comment {var-string}
        set type [application|category]
    next
end

```

config application group

Parameter	Description	Type	Size
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

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

Option	Description
<i>application</i>	Application ID.
<i>category</i>	Application category ID.

config application list

Configure application control lists.

```
config application list
    Description: Configure application control lists.
    edit <name>
        set app-replacemsg [disable|enable]
        set comment {var-string}
        set control-default-network-services [disable|enable]
        set deep-app-inspection [disable|enable]
        config default-network-services
            Description: Default network service entries.
            edit <id>
                set port {integer}
                set services {option1}, {option2}, ...
                set violation-action [pass|monitor|...]
            next
        end
        set enforce-default-app-port [disable|enable]
        config entries
            Description: Application list entries.
            edit <id>
                set action [pass|block|...]
                set application <id1>, <id2>, ...
                set behavior {user}
                set category <id1>, <id2>, ...
                set exclusion <id1>, <id2>, ...
                set log [disable|enable]
                set log-packet [disable|enable]
                config parameters
                    Description: Application parameters.
                    edit <id>
                        set value {string}
                    next
                end
                set per-ip-shaper {string}
                set popularity {option1}, {option2}, ...
```

```

        set protocols {user}
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        set risk <level1>, <level2>, ...
        set session-ttl {integer}
        set shaper {string}
        set shaper-reverse {string}
        set sub-category <id1>, <id2>, ...
        set technology {user}
        set vendor {user}
    next
end
set extended-log [enable|disable]
set force-inclusion-ssl-di-sigs [disable|enable]
set options {option1}, {option2}, ...
set other-application-action [pass|block]
set other-application-log [disable|enable]
set p2p-black-list {option1}, {option2}, ...
set replacemsg-group {string}
set unknown-application-action [pass|block]
set unknown-application-log [disable|enable]
next
end

```

config application list

Parameter	Description	Type	Size
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-
	Option	Description	
	<i>disable</i>	Disable replacement messages for blocked applications.	
	<i>enable</i>	Enable replacement messages for blocked applications.	
comment	comments	var-string	Maximum length: 255
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-
	Option	Description	
	<i>disable</i>	Disable protocol enforcement over selected ports.	
	<i>enable</i>	Enable protocol enforcement over selected ports.	

Parameter	Description	Type	Size								
deep-app-inspection	Enable/disable deep application inspection.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable deep application inspection.</td></tr><tr><td><i>enable</i></td><td>Enable deep application inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable deep application inspection.	<i>enable</i>	Enable deep application inspection.				
Option	Description										
<i>disable</i>	Disable deep application inspection.										
<i>enable</i>	Enable deep application inspection.										
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable default application port enforcement.</td></tr><tr><td><i>enable</i></td><td>Enable default application port enforcement.</td></tr></table>	Option	Description	<i>disable</i>	Disable default application port enforcement.	<i>enable</i>	Enable default application port enforcement.				
Option	Description										
<i>disable</i>	Disable default application port enforcement.										
<i>enable</i>	Enable default application port enforcement.										
extended-log	Enable/disable extended logging.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable forced inclusion of signatures which normally require SSL deep inspection.</td></tr><tr><td><i>enable</i></td><td>Enable forced inclusion of signatures which normally require SSL deep inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.	<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.				
Option	Description										
<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.										
<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.										
name	List name.	string	Maximum length: 35								
options	Basic application protocol signatures allowed by default.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow-dns</i></td><td>Allow DNS.</td></tr><tr><td><i>allow-icmp</i></td><td>Allow ICMP.</td></tr><tr><td><i>allow-http</i></td><td>Allow generic HTTP web browsing.</td></tr></table>	Option	Description	<i>allow-dns</i>	Allow DNS.	<i>allow-icmp</i>	Allow ICMP.	<i>allow-http</i>	Allow generic HTTP web browsing.		
Option	Description										
<i>allow-dns</i>	Allow DNS.										
<i>allow-icmp</i>	Allow ICMP.										
<i>allow-http</i>	Allow generic HTTP web browsing.										

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

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable logging for unknown applications.	
	<i>enable</i>	Enable logging for unknown applications.	

config default-network-services

Parameter	Description	Type	Size
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
port	Port number.	integer	Minimum value: 0 Maximum value: 65535
services	Network protocols.	option	-
	Option	Description	
	<i>http</i>	HTTP.	
	<i>ssh</i>	SSH.	
	<i>telnet</i>	TELNET.	
	<i>ftp</i>	FTP.	
	<i>dns</i>	DNS.	
	<i>smtp</i>	SMTP.	
	<i>pop3</i>	POP3.	
	<i>imap</i>	IMAP.	
	<i>snmp</i>	SNMP.	
	<i>nntp</i>	NNTP.	
	<i>https</i>	HTTPS.	
violation-action	Action for protocols not white listed under selected port.	option	-
	Option	Description	
	<i>pass</i>	Allow protocols not white listed under selected port.	

Parameter	Description	Type	Size
	Option	Description	
	<i>monitor</i>	Monitor protocols not white listed under selected port.	
	<i>block</i>	Block protocols not white listed under selected port.	

config entries

Parameter	Description	Type	Size
action	Pass or block traffic, or reset connection for traffic from this application.	option	-
	Option	Description	
	<i>pass</i>	Pass or allow matching traffic.	
	<i>block</i>	Block or drop matching traffic.	
	<i>reset</i>	Reset sessions for matching traffic.	
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295
behavior	Application behavior filter.	user	Not Specified
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
log	Enable/disable logging for this application list.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable logging.	
	<i>enable</i>	Enable logging.	
log-packet	Enable/disable packet logging.	option	-
	Option	Description	
	<i>disable</i>	Disable packet logging.	
	<i>enable</i>	Enable packet logging.	
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35
popularity	Application popularity filter (1 - 5, from least to most popular).	option	-
	Option	Description	
	<i>1</i>	Popularity level 1.	
	<i>2</i>	Popularity level 2.	
	<i>3</i>	Popularity level 3.	
	<i>4</i>	Popularity level 4.	
	<i>5</i>	Popularity level 5.	
protocols	Application protocol filter.	user	Not Specified
quarantine	Quarantine method.	option	-
	Option	Description	
	<i>none</i>	Quarantine is disabled.	
	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.	
quarantine-expiry	Duration of quarantine. (Format ###d###h###m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-
	Option	Description	
	<i>disable</i>	Disable quarantine logging.	
	<i>enable</i>	Enable quarantine logging.	

Parameter	Description	Type	Size												
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	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>Allow configured number of packets every rate-duration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once the rate is reached.</td></tr></table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.								
Option	Description														
<i>periodical</i>	Allow configured number of packets every rate-duration.														
<i>continuous</i>	Block packets once the rate is reached.														
rate-track	Track the packet protocol field.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>none</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr><tr><td><i>dhcp-client-mac</i></td><td>DHCP client.</td></tr><tr><td><i>dns-domain</i></td><td>DNS domain.</td></tr></table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.		
Option	Description														
<i>none</i>	none														
<i>src-ip</i>	Source IP.														
<i>dest-ip</i>	Destination IP.														
<i>dhcp-client-mac</i>	DHCP client.														
<i>dns-domain</i>	DNS domain.														
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295												
session-ttl	Session TTL (0 = default).	integer	Minimum value: 0 Maximum value: 4294967295												
shaper	Traffic shaper.	string	Maximum length: 35												
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35												

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

config parameters

Parameter	Description	Type	Size
id	Parameter ID.	integer	Minimum value: 0 Maximum value: 4294967295
value	Parameter value.	string	Maximum length: 63

config application name

Configure application signatures. Read-only.

```

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

```

config application name

Parameter	Description	Type	Size
behavior	Application behavior. Read-only.	user	Not Specified
category	Application category ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
id	Application ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
name	Application name.	string	Maximum length: 63
parameter	Application parameter name. Read-only.	string	Maximum length: 35
popularity	Application popularity. Read-only.	integer	Minimum value: 0 Maximum value: 255
protocol	Application protocol. Read-only.	user	Not Specified
risk	Application risk. Read-only.	integer	Minimum value: 0 Maximum value: 255
sub-category	Application sub-category ID. Read-only.	integer	Minimum value: 0 Maximum value: 255
technology	Application technology. Read-only.	user	Not Specified
vendor	Application vendor. Read-only.	user	Not Specified
weight	Application weight. Read-only.	integer	Minimum value: 0 Maximum value: 255

config metadata

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

config application rule-settings

Configure application rule settings. Read-only.

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

config application rule-settings

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

authentication

This section includes syntax for the following commands:

- [config authentication rule on page 70](#)
- [config authentication scheme on page 72](#)
- [config authentication setting on page 74](#)

config authentication rule

Configure Authentication Rules.

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

config authentication rule

Parameter	Description	Type	Size
active-auth-method	Select an active authentication method.	string	Maximum length: 35
comments	Comment.	var-string	Maximum length: 1023
ip-based	Enable/disable IP-based authentication. Once a user authenticates all traffic from the IP address the user authenticated from is allowed.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP-based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IP-based authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP-based authentication.	<i>disable</i>	Disable IP-based authentication.						
Option	Description												
<i>enable</i>	Enable IP-based authentication.												
<i>disable</i>	Disable IP-based authentication.												
name	Authentication rule name.	string	Maximum length: 35										
protocol	Select the protocol to use for authentication (default = http). Users connect to the FortiGate using this protocol and are asked to authenticate.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Use HTTP for authentication.</td></tr><tr><td><i>ftp</i></td><td>Use FTP for authentication.</td></tr><tr><td><i>socks</i></td><td>Use SOCKS for authentication.</td></tr><tr><td><i>ssh</i></td><td>Use SSH for authentication.</td></tr></table>	Option	Description	<i>http</i>	Use HTTP for authentication.	<i>ftp</i>	Use FTP for authentication.	<i>socks</i>	Use SOCKS for authentication.	<i>ssh</i>	Use SSH for authentication.		
Option	Description												
<i>http</i>	Use HTTP for authentication.												
<i>ftp</i>	Use FTP for authentication.												
<i>socks</i>	Use SOCKS for authentication.												
<i>ssh</i>	Use SSH for authentication.												
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										
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35										
status	Enable/disable this authentication rule.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this authentication rule.</td></tr><tr><td><i>disable</i></td><td>Disable this authentication rule.</td></tr></table>	Option	Description	<i>enable</i>	Enable this authentication rule.	<i>disable</i>	Disable this authentication rule.						
Option	Description												
<i>enable</i>	Enable this authentication rule.												
<i>disable</i>	Disable this authentication rule.												
transaction-based	Enable/disable transaction based authentication (default = disable).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable transaction based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable transaction based authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable transaction based authentication.	<i>disable</i>	Disable transaction based authentication.						
Option	Description												
<i>enable</i>	Enable transaction based authentication.												
<i>disable</i>	Disable transaction based authentication.												
web-auth-cookie	Enable/disable Web authentication cookies (default = disable).	option	-										

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

config authentication scheme

Configure Authentication Schemes.

```
config authentication scheme
    Description: Configure Authentication Schemes.
    edit <name>
        set domain-controller {string}
        set fsso-agent-for-ntlm {string}
        set fsso-guest [enable|disable]
        set kerberos-keytab {string}
        set method {option1}, {option2}, ...
        set negotiate-ntlm [enable|disable]
        set require-tfa [enable|disable]
        set ssh-ca {string}
        set user-database <name1>, <name2>, ...
    next
end
```

config authentication scheme

Parameter	Description	Type	Size
domain-controller	Domain controller setting.	string	Maximum length: 35
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35
fsso-guest	Enable/disable user fsso-guest authentication (default = disable).	option	-

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user fsso-guest authentication.</td></tr><tr><td><i>disable</i></td><td>Disable user fsso-guest authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable user fsso-guest authentication.	<i>disable</i>	Disable user fsso-guest authentication.														
	Option	Description																			
	<i>enable</i>	Enable user fsso-guest authentication.																			
<i>disable</i>	Disable user fsso-guest authentication.																				
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35																		
method	Authentication methods (default = basic).	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>digest</i></td><td>Digest HTTP authentication.</td></tr><tr><td><i>form</i></td><td>Form-based HTTP authentication.</td></tr><tr><td><i>negotiate</i></td><td>Negotiate authentication.</td></tr><tr><td><i>fsso</i></td><td>Fortinet Single Sign-On (FSSO) authentication.</td></tr><tr><td><i>rssso</i></td><td>RADIUS Single Sign-On (RSSO) authentication.</td></tr><tr><td><i>ssh-publickey</i></td><td>Public key based SSH authentication.</td></tr></table>	Option	Description	<i>ntlm</i>	NTLM authentication.	<i>basic</i>	Basic HTTP authentication.	<i>digest</i>	Digest HTTP authentication.	<i>form</i>	Form-based HTTP authentication.	<i>negotiate</i>	Negotiate authentication.	<i>fsso</i>	Fortinet Single Sign-On (FSSO) authentication.	<i>rssso</i>	RADIUS Single Sign-On (RSSO) authentication.	<i>ssh-publickey</i>	Public key based SSH authentication.		
	Option	Description																			
	<i>ntlm</i>	NTLM authentication.																			
	<i>basic</i>	Basic HTTP authentication.																			
	<i>digest</i>	Digest HTTP authentication.																			
	<i>form</i>	Form-based HTTP authentication.																			
	<i>negotiate</i>	Negotiate authentication.																			
	<i>fsso</i>	Fortinet Single Sign-On (FSSO) authentication.																			
<i>rssso</i>	RADIUS Single Sign-On (RSSO) authentication.																				
<i>ssh-publickey</i>	Public key based SSH authentication.																				
name	Authentication scheme name.	string	Maximum length: 35																		
negotiate-ntlm	Enable/disable negotiate authentication for NTLM (default = disable).	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negotiate authentication for NTLM.</td></tr><tr><td><i>disable</i></td><td>Disable negotiate authentication for NTLM.</td></tr></table>	Option	Description	<i>enable</i>	Enable negotiate authentication for NTLM.	<i>disable</i>	Disable negotiate authentication for NTLM.														
	Option	Description																			
	<i>enable</i>	Enable negotiate authentication for NTLM.																			
<i>disable</i>	Disable negotiate authentication for NTLM.																				
require-tfa	Enable/disable two-factor authentication (default = disable).	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable two-factor authentication.</td></tr><tr><td><i>disable</i></td><td>Disable two-factor authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable two-factor authentication.	<i>disable</i>	Disable two-factor authentication.														
	Option	Description																			
	<i>enable</i>	Enable two-factor authentication.																			
<i>disable</i>	Disable two-factor authentication.																				
ssh-ca	SSH CA name.	string	Maximum length: 35																		
user-database <name>	Authentication server to contain user information; "local" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79																		

config authentication setting

Configure authentication setting.

```
config authentication setting
    Description: Configure authentication setting.
    set active-auth-scheme {string}
    set auth-https [enable|disable]
    set captive-portal {string}
    set captive-portal-ip {ipv4-address-any}
    set captive-portal-ip6 {ipv6-address}
    set captive-portal-port {integer}
    set captive-portal-ssl-port {integer}
    set captive-portal-type [fqdn|ip]
    set captive-portal6 {string}
    set sso-auth-scheme {string}
end
```

config authentication setting

Parameter	Description	Type	Size
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
captive-portal	Captive portal host name.	string	Maximum length: 255
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-port	Captive portal port number (1 - 65535, default = 7830).	integer	Minimum value: 1 Maximum value: 65535

Parameter	Description	Type	Size
captive-portal-ssl-port	Captive portal SSL port number (1 - 65535, default = 7831).	integer	Minimum value: 1 Maximum value: 65535
captive-portal-type	Captive portal type.	option	-
	Option	Description	
	fqdn	Use FQDN for captive portal.	
	ip	Use an IP address for captive portal.	
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35

certificate

This section includes syntax for the following commands:

- [config certificate ca](#) on page 76
- [config certificate crl](#) on page 77
- [config certificate local](#) on page 79
- [config certificate remote](#) on page 82

config certificate ca

CA certificate.

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

config certificate ca

Parameter	Description	Type	Size
auto-update-days	Number of days to wait before requesting an updated CA certificate (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295
auto-update-days-warning	Number of days before an expiry-warning message is generated (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295
ca	CA certificate as a PEM file.	user	Not Specified

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 79
range	Either global or VDOM IP address range for the CA certificate.	option	-
	Option	Description	
	<i>global</i>	Global range.	
	<i>vdom</i>	VDOM IP address range.	
scep-url	URL of the SCEP server.	string	Maximum length: 255
source	CA certificate source type.	option	-
	Option	Description	
	<i>factory</i>	Factory installed certificate.	
	<i>user</i>	User generated certificate.	
	<i>bundle</i>	Bundle file certificate.	
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-
	Option	Description	
	<i>enable</i>	Trusted CA for SSL inspection.	
	<i>disable</i>	Untrusted CA for SSL inspection.	

config certificate crl

Certificate Revocation List as a PEM file.

```

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

```

```

        set source-ip {ipv4-address}
        set update-interval {integer}
        set update-vdom {string}
    next
end

```

config certificate crl

Parameter	Description	Type	Size
crl	Certificate Revocation List as a PEM file.	user	Not Specified
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255
ldap-password	LDAP server user password.	password	Not Specified
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35
ldap-username	LDAP server user name.	string	Maximum length: 63
name	Name.	string	Maximum length: 35
range	Either global or VDOM IP address range for the certificate.	option	-

Option	Description
<i>global</i>	Global range.
<i>vdom</i>	VDOM IP address range.

scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255
source	Certificate source type.	option	-

Option	Description
<i>factory</i>	Factory installed certificate.
<i>user</i>	User generated certificate.
<i>bundle</i>	Bundle file certificate.

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

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
update-vdom	VDOM for CRL update.	string	Maximum length: 31

config certificate local

Local keys and certificates.

```

config certificate local
    Description: Local keys and certificates.
    edit <name>
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set ca-identifier {string}
        set certificate {user}
        set cmp-path {string}
        set cmp-regeneration-method [keyupdate|renewal]
        set cmp-server {string}
        set cmp-server-cert {string}
        set comments {string}
        set csr {user}
        set enroll-protocol [none|scep|...]
        set ike-localid {string}
        set ike-localid-type [asn1dn|fqdn]
        set name-encoding [printable|utf8]
        set password {password}
        set private-key {user}
        set range [global|vdom]
        set scep-password {password}
        set scep-url {string}
        set source [factory|user|...]
        set source-ip {ipv4-address}
        set state {user}
    next
end

```

config certificate local

Parameter	Description	Type	Size
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
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255
certificate	PEM format certificate.	user	Not Specified
cmp-path	Path location inside CMP server.	string	Maximum length: 255
cmp-regeneration-method	CMP auto-regeneration method.	option	-

Option	Description
<i>keyupdate</i>	Key Update.
<i>renewal</i>	Renewal.

cmp-server	'ADDRESS:PORT' for CMP server.	string	Maximum length: 63
cmp-server-cert	CMP server certificate.	string	Maximum length: 79
comments	Comment.	string	Maximum length: 511
csr	Certificate Signing Request.	user	Not Specified
enroll-protocol	Certificate enrollment protocol.	option	-

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

Parameter	Description	Type	Size
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.	
name	Name.	string	Maximum length: 35
name-encoding	Name encoding method for auto-regeneration.	option	-
	Option	Description	
	printable	Printable encoding (default).	
	utf8	UTF-8 encoding.	
password	Password as a PEM file.	password	Not Specified
private-key	PEM format key, encrypted with a password.	user	Not Specified
range	Either a global or VDOM IP address range for the certificate.	option	-
	Option	Description	
	global	Global range.	
	vdom	VDOM IP address range.	
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified
scep-url	SCEP server URL.	string	Maximum length: 255
source	Certificate source type.	option	-
	Option	Description	
	factory	Factory installed certificate.	
	user	User generated certificate.	
	bundle	Bundle file certificate.	
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified
state	Certificate Signing Request State. Read-only.	user	Not Specified

config certificate remote

Remote certificate as a PEM file.

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

config certificate remote

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

cifs

This section includes syntax for the following commands:

- [config cifs domain-controller on page 83](#)
- [config cifs profile on page 84](#)

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 ip {ipv4-address-any}
        set ip6 {ipv6-address}
        set password {password}
        set port {integer}
        set username {string}
    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
ip	IPv4 server address.	ipv4-address-any	Not Specified
ip6	IPv6 server address.	ipv6-address	Not Specified
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
server-name	Name of the server to connect to.	string	Maximum length: 255
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64

config cifs profile

Configure CIFS profile.

```
config cifs profile
  Description: Configure CIFS profile.
  edit <name>
    set domain-controller {string}
    config file-filter
      Description: File filter.
      config entries
        Description: File filter entries.
        edit <filter>
          set action [log|block]
          set comment {var-string}
          set direction [incoming|outgoing|...]
          set file-type <name1>, <name2>, ...
        next
      end
    set log [enable|disable]
    set status [enable|disable]
  end
  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
name	Profile name.	string	Maximum length: 35
server-credential-type	CIFS server credential type.	option	-

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

config file-filter

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

config entries

Parameter	Description	Type	Size
action	Action taken for matched file.	option	-
	Option	Description	
	<i>log</i>	Allow the content and write a log message.	
	<i>block</i>	Block the content and write a log message.	
comment	Comment.	var-string	Maximum length: 255
direction	Match files transmitted in the session's originating or reply direction.	option	-
	Option	Description	
	<i>incoming</i>	Match files transmitted in the session's originating direction.	
	<i>outgoing</i>	Match files transmitted in the session's reply direction.	
	<i>any</i>	Match files transmitted in the session's originating and reply direction.	
file-type <name>	Select file type. File type name.	string	Maximum length: 39
filter	Add a file filter.	string	Maximum length: 35

config server-keytab

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

dlp

This section includes syntax for the following commands:

- [config dlp filepattern on page 87](#)
- [config dlp fp-doc-source on page 90](#)
- [config dlp sensitivity on page 93](#)
- [config dlp sensor on page 94](#)
- [config dlp settings on page 99](#)

config dlp filepattern

Configure file patterns used by DLP blocking.

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

config dlp filepattern

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

config entries

Parameter	Description	Type	Size
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.	

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>iso</i></td><td>Match ISO archive files.</td></tr><tr><td><i>crx</i></td><td>Match Chrome extension files.</td></tr><tr><td><i>flac</i></td><td>Match flac files.</td></tr></table>	Option	Description	<i>iso</i>	Match ISO archive files.	<i>crx</i>	Match Chrome extension files.	<i>flac</i>	Match flac files.		
	Option	Description									
	<i>iso</i>	Match ISO archive files.									
	<i>crx</i>	Match Chrome extension files.									
<i>flac</i>	Match flac files.										
filter-type	Filter by file name pattern or by file type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pattern</i></td><td>Filter by file name pattern.</td></tr><tr><td><i>type</i></td><td>Filter by file type.</td></tr></table>	Option	Description	<i>pattern</i>	Filter by file name pattern.	<i>type</i>	Filter by file type.				
	Option	Description									
	<i>pattern</i>	Filter by file name pattern.									
<i>type</i>	Filter by file type.										
pattern	Add a file name pattern.	string	Maximum length: 79								

config dlp fp-doc-source



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 51E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E.

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

```

config dlp fp-doc-source
    Description: Create a DLP fingerprint database by allowing the FortiGate to access a
    file server containing files from which to create fingerprints.
    edit <name>
        set date {integer}
        set file-path {string}
        set file-pattern {string}
        set keep-modified [enable|disable]
        set password {password}
        set period [none|daily|...]
        set remove-deleted [enable|disable]
        set scan-on-creation [enable|disable]
        set scan-subdirectories [enable|disable]
        set sensitivity {string}
        set server {string}
        set server-type {option}
        set tod-hour {integer}
        set tod-min {integer}
        set username {string}
        set vdom [mgmt|current]
        set weekday [sunday|monday|...]
    next
end

```

config dlp fp-doc-source

Parameter	Description	Type	Size						
date	Day of the month on which to scan the server (1 - 31).	integer	Minimum value: 1 Maximum value: 31						
file-path	Path on the server to the fingerprint files (max 119 characters).	string	Maximum length: 119						
file-pattern	Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards.	string	Maximum length: 35						
keep-modified	Enable so that when a file is changed on the server the FortiGate keeps the old fingerprint and adds a new fingerprint to the database.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the old fingerprint and add a new fingerprint when a file is changed on the server.</td></tr><tr><td><i>disable</i></td><td>Replace the old fingerprint with the new fingerprint when a file is changed on the server.</td></tr></table>	Option	Description	<i>enable</i>	Keep the old fingerprint and add a new fingerprint when a file is changed on the server.	<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.		
Option	Description								
<i>enable</i>	Keep the old fingerprint and add a new fingerprint when a file is changed on the server.								
<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.								
name	Name of the DLP fingerprint database.	string	Maximum length: 35						

Parameter	Description	Type	Size										
password	Password required to log into the file server.	password	Not Specified										
period	Frequency for which the FortiGate checks the server for new or changed files.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Check the server when the FortiGate starts up.</td></tr><tr><td><i>daily</i></td><td>Check the server once a day.</td></tr><tr><td><i>weekly</i></td><td>Check the server once a week.</td></tr><tr><td><i>monthly</i></td><td>Check the server once a month.</td></tr></table>	Option	Description	<i>none</i>	Check the server when the FortiGate starts up.	<i>daily</i>	Check the server once a day.	<i>weekly</i>	Check the server once a week.	<i>monthly</i>	Check the server once a month.		
Option	Description												
<i>none</i>	Check the server when the FortiGate starts up.												
<i>daily</i>	Check the server once a day.												
<i>weekly</i>	Check the server once a week.												
<i>monthly</i>	Check the server once a month.												
remove-deleted	Enable to keep the fingerprint database up to date when a file is deleted from the server.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the fingerprint database up to date when a file is deleted from server.</td></tr><tr><td><i>disable</i></td><td>Do not check for deleted files on the server. Saves system resources.</td></tr></table>	Option	Description	<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from server.	<i>disable</i>	Do not check for deleted files on the server. Saves system resources.						
Option	Description												
<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from server.												
<i>disable</i>	Do not check for deleted files on the server. Saves system resources.												
scan-on-creation	Enable to keep the fingerprint database up to date when a file is added or changed on the server.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the fingerprint database up to date when a file is added or changed on the server.</td></tr><tr><td><i>disable</i></td><td>Do not check for added or changed files on the server. Saves system resources.</td></tr></table>	Option	Description	<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.	<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.						
Option	Description												
<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.												
<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.												
scan-subdirectories	Enable/disable scanning subdirectories to find files to create fingerprints from.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Scan subdirectories.</td></tr><tr><td><i>disable</i></td><td>Do not scan subdirectories.</td></tr></table>	Option	Description	<i>enable</i>	Scan subdirectories.	<i>disable</i>	Do not scan subdirectories.						
Option	Description												
<i>enable</i>	Scan subdirectories.												
<i>disable</i>	Do not scan subdirectories.												
sensitivity	Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using sensitivity.	string	Maximum length: 35										
server	IPv4 or IPv6 address of the server.	string	Maximum length: 35										

Parameter	Description	Type	Size
server-type	Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.	option	-
	Option	Description	
	<i>samba</i>	SAMBA server.	
tod-hour	Hour of the day on which to scan the server (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23
tod-min	Minute of the hour on which to scan the server (0 - 59).	integer	Minimum value: 0 Maximum value: 59
username	User name required to log into the file server.	string	Maximum length: 35
vdom	Select the VDOM that can communicate with the file server.	option	-

Option	Description
<i>mgmt</i>	Communicate with the file server through the management VDOM.
<i>current</i>	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.

weekday	Day of the week on which to scan the server.	option	-
	Option	Description	
	<i>sunday</i>	Sunday	
	<i>monday</i>	Monday	
	<i>tuesday</i>	Tuesday	
	<i>wednesday</i>	Wednesday	
	<i>thursday</i>	Thursday	
	<i>friday</i>	Friday	
	<i>saturday</i>	Saturday	

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
end

```

config dlp sensitivity

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

config dlp sensor

Configure DLP sensors.

```

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

```

config dlp sensor

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
dlp-log	Enable/disable DLP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP logging.	
	<i>disable</i>	Disable DLP logging.	
extended-log	Enable/disable extended logging for data leak prevention.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
full-archive-proto	Protocols to always content archive.	option	-
	Option	Description	
	<i>smtp</i>	SMTP.	
	<i>pop3</i>	POP3.	
	<i>imap</i>	IMAP.	
	<i>http-get</i>	HTTP GET.	
	<i>http-post</i>	HTTP POST.	
	<i>ftp</i>	FTP.	
	<i>nntp</i>	NNTP.	
	<i>mapi</i>	MAPI.	
<i>ssh</i>	SFTP and SCP.		
nac-quar-log	Enable/disable NAC quarantine logging.	option	-
	Option	Description	
	<i>enable</i>	Enable NAC quarantine logging.	
	<i>disable</i>	Disable NAC quarantine logging.	
name	Name of the DLP sensor.	string	Maximum length: 35

Parameter	Description	Type	Size
options	Configure DLP options.	option	-
replacemsg-group	Replacement message group used by this DLP sensor.	string	Maximum length: 35
summary-proto	Protocols to always log summary.	option	-

Option	Description
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>imap</i>	IMAP.
<i>http-get</i>	HTTP GET.
<i>http-post</i>	HTTP POST.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>mapi</i>	MAPI.
<i>ssh</i>	SFTP and SCP.

config filter

Parameter	Description	Type	Size
action	Action to take with content that this DLP sensor matches.	option	-

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

archive	Enable/disable DLP archiving.	option	-

Option	Description
<i>disable</i>	No DLP archiving.
<i>enable</i>	Enable full DLP archiving.

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																		
expiry	Quarantine duration in days, hours, minutes format (dddhhmm).	user	Not Specified																		
file-size	Match files this size or larger (0 - 4294967295 kbytes).	integer	Minimum value: 0 Maximum value: 4294967295																		
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295																		
filter-by	Select the type of content to match.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>credit-card</td><td>Match credit cards.</td></tr><tr><td>ssn</td><td>Match social security numbers.</td></tr><tr><td>regex</td><td>Use a regular expression to match content.</td></tr><tr><td>file-type</td><td>Match a DLP file pattern list.</td></tr><tr><td>file-size</td><td>Match any file over with a size over the threshold.</td></tr><tr><td>fingerprint</td><td>Match against a fingerprint sensitivity.</td></tr><tr><td>watermark</td><td>Look for defined file watermarks.</td></tr><tr><td>encrypted</td><td>Look for encrypted files.</td></tr></table>			Option	Description	credit-card	Match credit cards.	ssn	Match social security numbers.	regex	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.	fingerprint	Match against a fingerprint sensitivity.	watermark	Look for defined file watermarks.	encrypted	Look for encrypted files.
	Option	Description																			
	credit-card	Match credit cards.																			
	ssn	Match social security numbers.																			
	regex	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.																			
	fingerprint	Match against a fingerprint sensitivity.																			
	watermark	Look for defined file watermarks.																			
encrypted	Look for encrypted files.																				
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295																		
match-percentage *	Percentage of fingerprints in the fingerprint databases designated with the selected sensitivity to match.	integer	Minimum value: 1 Maximum value: 100																		
name	Filter name.	string	Maximum length: 35																		

Parameter	Description	Type	Size
proto	Check messages or files over one or more of these protocols.	option	-

Option	Description
<i>smtp</i>	SMTP.
<i>pop3</i>	POP3.
<i>imap</i>	IMAP.
<i>http-get</i>	HTTP GET.
<i>http-post</i>	HTTP POST.
<i>ftp</i>	FTP.
<i>nntp</i>	NNTP.
<i>mapi</i>	MAPI.
<i>ssh</i>	SFTP and SCP.

regexp	Enter a regular expression to match (max. 255 characters).	string	Maximum length: 255
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35
severity	Select the severity or threat level that matches this filter.	option	-

Option	Description
<i>info</i>	Informational.
<i>low</i>	Low.
<i>medium</i>	Medium.
<i>high</i>	High.
<i>critical</i>	Critical.

type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-

Option	Description
<i>file</i>	Check the contents of downloaded or attached files.
<i>message</i>	Check the contents of email messages, web pages, etc.

* This parameter may not exist in some models.

config dlp settings



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 51E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E.

Designate logical storage for DLP fingerprint database.

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

config dlp settings

Parameter	Description	Type	Size
cache-mem-percent	Maximum percentage of available memory allocated to caching (1 - 15%).	integer	Minimum value: 1 Maximum value: 15

Parameter	Description	Type	Size
chunk-size	Maximum fingerprint chunk size. **Changing will flush the entire database** .	integer	Minimum value: 100 Maximum value: 100000
db-mode	Behaviour when the maximum size is reached.	option	-
	Option	Description	
	<i>stop-adding</i>	Stop adding entries.	
	<i>remove-modified-then-oldest</i>	Remove modified chunks first, then oldest file entries.	
	<i>remove-oldest</i>	Remove the oldest files first.	
size	Maximum total size of files within the storage (MB).	integer	Minimum value: 16 Maximum value: 4294967295
storage-device	Storage device name.	string	Maximum length: 35

dnsfilter

This section includes syntax for the following commands:

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

config dnsfilter domain-filter

Configure DNS domain filters.

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

config dnsfilter domain-filter

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

config entries

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

config dnsfilter profile

Configure DNS domain filter profiles.

```
config dnsfilter profile
  Description: Configure DNS domain filter profiles.
  edit <name>
    set block-action [block|redirect]
    set block-botnet [disable|enable]
    set comment {var-string}
    config dns-translation
      Description: DNS translation settings.
      edit <id>
        set addr-type [ipv4|ipv6]
```

```

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

```

config dnsfilter profile

Parameter	Description	Type	Size						
block-action	Action to take for blocked domains.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Return NXDOMAIN for blocked domains.</td></tr><tr><td><i>redirect</i></td><td>Redirect blocked domains to SDNS portal.</td></tr></table>			Option	Description	<i>block</i>	Return NXDOMAIN for blocked domains.	<i>redirect</i>	Redirect blocked domains to SDNS portal.
Option	Description								
<i>block</i>	Return NXDOMAIN for blocked domains.								
<i>redirect</i>	Redirect blocked domains to SDNS portal.								
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable blocking botnet C&C DNS lookups.</td></tr><tr><td><i>enable</i></td><td>Enable blocking botnet C&C DNS lookups.</td></tr></table>			Option	Description	<i>disable</i>	Disable blocking botnet C&C DNS lookups.	<i>enable</i>	Enable blocking botnet C&C DNS lookups.
Option	Description								
<i>disable</i>	Disable blocking botnet C&C DNS lookups.								
<i>enable</i>	Enable blocking botnet C&C DNS lookups.								

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-

Option	Description

<i>enable</i>	Enable logging of all domains visited.

<i>disable</i>	Disable logging of all domains visited.

name	Profile name.	string	Maximum length: 35
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
safe-search	Enable/disable Google, Bing, and YouTube safe search.	option	-

Option	Description

<i>disable</i>	Disable Google, Bing, and YouTube safe search.

<i>enable</i>	Enable Google, Bing, and YouTube safe search.

sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-

Option	Description

<i>enable</i>	Enable domain filtering and botnet domain logging.

<i>disable</i>	Disable domain filtering and botnet domain logging.

Option	Description

<i>enable</i>	Enable FortiGuard SDNS rating error logging.

<i>disable</i>	Disable FortiGuard SDNS rating error logging.

youtube-restrict	Set safe search for YouTube restriction level.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>strict</i>	Enable strict safe search for YouTube.	
	<i>moderate</i>	Enable moderate safe search for YouTube.	

config dns-translation

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

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	
	<i>error-allow</i>	Allow all domains when FortiGuard DNS servers fail.	
	<i>ftgd-disable</i>	Disable FortiGuard DNS domain rating.	

config filters

Parameter	Description	Type	Size
action	Action to take for DNS requests matching the category.	option	-
	Option	Description	
	<i>block</i>	Block DNS requests matching the category.	
	<i>monitor</i>	Allow DNS requests matching the category and log the result.	

Parameter	Description	Type	Size
category	Category number.	integer	Minimum value: 0 Maximum value: 255
id	ID number.	integer	Minimum value: 0 Maximum value: 255
log	Enable/disable DNS filter logging for this DNS profile.	option	-

Option	Description
<i>enable</i>	Enable DNS filter logging.
<i>disable</i>	Disable DNS filter logging.

dpdk

This section includes syntax for the following commands:

- [config dpdk cpus on page 108](#)
- [config dpdk global on page 109](#)

config dpdk cpus



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

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure CPUs enabled to run engines in each DPDK stage.

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

config dpdk cpus

Parameter	Description	Type	Size
ips-cpus	CPUs enabled to run DPDK IPS engines.	string	Maximum length: 1022
rx-cpus	CPUs enabled to run DPDK RX engines.	string	Maximum length: 1022
tx-cpus	CPUs enabled to run DPDK TX engines.	string	Maximum length: 1022
vnp-cpus	CPUs enabled to run DPDK VNP engines.	string	Maximum length: 1022

config dpdk global



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

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure global DPDK options.

```
config dpdk global
  Description: Configure global DPDK options.
  set elasticbuffer [disable|enable]
  set hugepage-percentage {integer}
  set interface <interface-name1>, <interface-name2>, ...
```

```

set mbufpool-percentage {integer}
set multiqueue [disable|enable]
set per-session-accounting [disable|traffic-log-only|...]
set sleep-on-idle [disable|enable]
set status [disable|enable]

```

end

config dpdk global

Parameter	Description	Type	Size
elasticbuffer	Enable/disable elasticbuffer support for all DPDK ports.	option	-
	Option	Description	
	<i>disable</i>	Disable elasticbuffer support for DPDK ports.	
	<i>enable</i>	Enable elasticbuffer support for DPDK ports.	
hugepage-percentage	Percentage of main memory allocated to hugepages, which are available for DPDK operation.	integer	Minimum value: 10 Maximum value: 50
interface <interface-name>	Physical interfaces that enable DPDK. Physical interface name.	string	Maximum length: 31
mbufpool-percentage	Percentage of main memory allocated to DPDK packet buffer.	integer	Minimum value: 5 Maximum value: 45
multiqueue	Enable/disable multi-queue RX/TX support for all DPDK ports.	option	-
	Option	Description	
	<i>disable</i>	Disable multi-queue RX/TX support for DPDK ports.	
	<i>enable</i>	Enable multi-queue RX/TX support for DPDK ports.	
per-session-accounting	Enable/disable per-session accounting.	option	-
	Option	Description	
	<i>disable</i>	Disable per-session accounting.	
	<i>traffic-log-only</i>	Enable per-session accounting only for VNP sessions with traffic logging turned on in firewall policy.	
	<i>enable</i>	Enable per-session accounting for all VNP sessions. *Affect performance.	

Parameter	Description	Type	Size						
sleep-on-idle	Enable/disable sleep-on-idle support for all FDH engines.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable sleep-on-idle support for FDH engines.</td></tr><tr><td><i>enable</i></td><td>Enable sleep-on-idle support for FDH engines.</td></tr></table>	Option	Description	<i>disable</i>	Disable sleep-on-idle support for FDH engines.	<i>enable</i>	Enable sleep-on-idle support for FDH engines.		
Option	Description								
<i>disable</i>	Disable sleep-on-idle support for FDH engines.								
<i>enable</i>	Enable sleep-on-idle support for FDH engines.								
status	Enable/disable DPDK operation for the entire system.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DPDK operation.</td></tr><tr><td><i>enable</i></td><td>Enable DPDK operation. *The minimum system requirements for DPDK are 2 vCPUs and 4GB memory.</td></tr></table>	Option	Description	<i>disable</i>	Disable DPDK operation.	<i>enable</i>	Enable DPDK operation. *The minimum system requirements for DPDK are 2 vCPUs and 4GB memory.		
Option	Description								
<i>disable</i>	Disable DPDK operation.								
<i>enable</i>	Enable DPDK operation. *The minimum system requirements for DPDK are 2 vCPUs and 4GB memory.								

emailfilter

This section includes syntax for the following commands:

- [config emailfilter bwl on page 112](#)
- [config emailfilter bword on page 114](#)
- [config emailfilter dnsbl on page 116](#)
- [config emailfilter fortishield on page 117](#)
- [config emailfilter iptrust on page 118](#)
- [config emailfilter mheader on page 119](#)
- [config emailfilter options on page 121](#)
- [config emailfilter profile on page 121](#)

config emailfilter bwl

Configure anti-spam black/white list.

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

config emailfilter bwl

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

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Name of table.	string	Maximum length: 63

config entries

Parameter	Description	Type	Size
action	Reject, mark as spam or good email.	option	-
	Option	Description	
	<i>reject</i>	Reject the connection.	
	<i>spam</i>	Mark as spam email.	
	<i>clear</i>	Mark as good email.	
addr-type	IP address type.	option	-
	Option	Description	
	<i>ipv4</i>	IPv4 Address type.	
	<i>ipv6</i>	IPv6 Address type.	
email-pattern	Email address pattern.	string	Maximum length: 127
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
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	
	<i>wildcard</i>	Wildcard pattern.	
	<i>regexp</i>	Perl regular expression.	
status	Enable/disable status.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable status.	
	<i>disable</i>	Disable status.	
type	Entry type.	option	-
	Option	Description	
	<i>ip</i>	By IP address.	
	<i>email</i>	By email address.	

config emailfilter bword

Configure AntiSpam banned word list.

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

config emailfilter bword

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

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Name of table.	string	Maximum length: 63

config entries

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

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

config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

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

config emailfilter dnsbl

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

config entries

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

config emailfilter fortishield

Configure FortiGuard - AntiSpam.

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

```

set spam-submit-srv {string}
set spam-submit-txt2htm [enable|disable]
end

```

config emailfilter fortishield

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

config emailfilter iptrust

Configure AntiSpam IP trust.

```

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

```

config emailfilter iptrust

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

config entries

Parameter	Description	Type	Size						
addr-type	Type of address.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 Address type.</td></tr><tr><td>ipv6</td><td>IPv6 Address type.</td></tr></table>			Option	Description	ipv4	IPv4 Address type.	ipv6	IPv6 Address type.
	Option	Description							
	ipv4	IPv4 Address type.							
ipv6	IPv6 Address type.								
id	Trusted IP entry ID.	integer	Minimum value: 0 Maximum value: 4294967295						
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						
status	Enable/disable status.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable status.</td></tr><tr><td>disable</td><td>Disable status.</td></tr></table>			Option	Description	enable	Enable status.	disable	Disable status.
	Option	Description							
	enable	Enable status.							
disable	Disable status.								

config emailfilter mheader

Configure AntiSpam MIME header.

```

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

```

config emailfilter mheader

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

config entries

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

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

config emailfilter options

Configure AntiSpam options.

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

config emailfilter options

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

config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
    Description: Configure Email Filter profiles.
    edit <name>
```

```

set comment {var-string}
set external [enable|disable]
config file-filter
    Description: File filter.
    config entries
        Description: File filter entries.
        edit <filter>
            set action [log|block]
            set comment {var-string}
            set file-type <name1>, <name2>, ...
            set password-protected [yes|any]
            set protocol {option1}, {option2}, ...
        next
    end
    set log [enable|disable]
    set scan-archive-contents [enable|disable]
    set status [enable|disable]
end
config gmail
    Description: Gmail.
    set log [enable|disable]
end
config imap
    Description: IMAP.
    set action [pass|tag]
    set log [enable|disable]
    set tag-msg {string}
    set tag-type {option1}, {option2}, ...
end
config mapi
    Description: MAPI.
    set action [pass|discard]
    set log [enable|disable]
end
config msn-hotmail
    Description: MSN Hotmail.
    set log [enable|disable]
end
set options {option1}, {option2}, ...
config pop3
    Description: POP3.
    set action [pass|tag]
    set log [enable|disable]
    set tag-msg {string}
    set tag-type {option1}, {option2}, ...
end
set replacemsg-group {string}
config smtp
    Description: SMTP.
    set action [pass|tag|...]
    set hdrip [disable|enable]
    set local-override [disable|enable]
    set log [enable|disable]
    set tag-msg {string}
    set tag-type {option1}, {option2}, ...
end

```

```

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

```

config emailfilter profile

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
external	Enable/disable external Email inspection.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

name	Profile name.	string	Maximum length: 35
options	Options.	option	-

Option	Description
<i>bannedword</i>	Content block.
<i>spambwl</i>	Black/white list.
<i>spamfsip</i>	Email IP address FortiGuard AntiSpam black list check.
<i>spamfssubmit</i>	Add FortiGuard AntiSpam spam submission text.
<i>spamfschksum</i>	Email checksum FortiGuard AntiSpam check.
<i>spamfsurl</i>	Email content URL FortiGuard AntiSpam check.
<i>spamhelodns</i>	Email helo/ehlo domain DNS check.
<i>spamraddrdns</i>	Email return address DNS check.
<i>spamrbl</i>	Email DNSBL & ORBL check.

Parameter	Description	Type	Size

Option	Description
<i>spamhdrcheck</i>	Email mime header check.
<i>spamfphish</i>	Email content phishing URL FortiGuard AntiSpam check.

replacemsg-group	Replacement message group.	string	Maximum length: 35
spam-bwl-table	Anti-spam black/white list table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647
spam-filtering	Enable/disable spam filtering.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 Maximum value: 4294967295
spam-log	Enable/disable spam logging for email filtering.	option	-

Option	Description
<i>disable</i>	Disable spam logging for email filtering.
<i>enable</i>	Enable spam logging for email filtering.

spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-

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

config file-filter

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

config entries

Parameter	Description	Type	Size								
action	Action taken for matched file.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log</td><td>Allow the content and write a log message.</td></tr><tr><td>block</td><td>Block the content and write a log message.</td></tr></table>	Option	Description	log	Allow the content and write a log message.	block	Block the content and write a log message.				
Option	Description										
log	Allow the content and write a log message.										
block	Block the content and write a log message.										
comment	Comment.	var-string	Maximum length: 255								
file-type <name>	Select file type. File type name.	string	Maximum length: 39								
filter	Add a file filter.	string	Maximum length: 35								
password-protected	Match password-protected files.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>yes</td><td>Match only password-protected files.</td></tr><tr><td>any</td><td>Match any file.</td></tr></table>	Option	Description	yes	Match only password-protected files.	any	Match any file.				
Option	Description										
yes	Match only password-protected files.										
any	Match any file.										
protocol	Protocols to apply with.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>smtp</td><td>Enable/disable SMTP.</td></tr><tr><td>imap</td><td>Enable/disable IMAP.</td></tr><tr><td>pop3</td><td>Enable/disable POP3.</td></tr></table>	Option	Description	smtp	Enable/disable SMTP.	imap	Enable/disable IMAP.	pop3	Enable/disable POP3.		
Option	Description										
smtp	Enable/disable SMTP.										
imap	Enable/disable IMAP.										
pop3	Enable/disable POP3.										

config gmail

Parameter	Description	Type	Size						
log	Enable/disable logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

config imap

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

config mapi

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

config msn-hotmail

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

config pop3

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

config smtp

Parameter	Description	Type	Size
action	Action for spam email.	option	-

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

config yahoo-mail

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

endpoint-control

This section includes syntax for the following commands:

- [config endpoint-control fctems on page 131](#)
- [config endpoint-control settings on page 132](#)

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

config endpoint-control fctems

Parameter	Description	Type	Size
admin-password	FortiClient EMS admin password.	password	Not Specified
admin-username	FortiClient EMS admin username.	string	Maximum length: 128
call-timeout	FortiClient EMS call timeout in milliseconds (500 - 30000 milliseconds, default = 5000).	integer	Minimum value: 500 Maximum value: 30000
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr><tr><td><i>disable</i></td><td>Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.	<i>disable</i>	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.		
	Option	Description							
	<i>enable</i>	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.							
<i>disable</i>	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.								
https-port	FortiClient EMS HTTPS access port number. (1 - 65535, default: 443).	integer	Minimum value: 1 Maximum value: 65535						
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35						
serial-number	FortiClient EMS Serial Number.	string	Maximum length: 16						
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255						
source-ip	REST API call source IP.	ipv4-address-any	Not Specified						

config endpoint-control settings

Configure endpoint control settings.

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

config endpoint-control settings

Parameter	Description	Type	Size
forticlient-disconnect-unsupported-client	Enable/disable disconnecting of unsupported FortiClient endpoints.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable disconnection of clients on unsupported routes.	
	<i>disable</i>	Disable disconnection of clients on unsupported routes.	
forticlient-keepalive-interval	Interval between two KeepAlive messages from FortiClient (20 - 300 sec, default = 60).	integer	Minimum value: 20 Maximum value: 300
forticlient-sys-update-interval	Interval between two system update messages from FortiClient (30 - 1440 min, default = 720).	integer	Minimum value: 30 Maximum value: 1440
forticlient-user-avatar	Enable/disable uploading FortiClient user avatars.	option	-
	Option	Description	
	<i>enable</i>	Allow uploading FortiClient user avatars.	
	<i>disable</i>	Disable uploading FortiClient user avatars.	

extender-controller

This section includes syntax for the following commands:

- [config extender-controller extender](#) on page 134

config extender-controller extender

Extender controller configuration.

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

next
end

config extender-controller extender

Parameter	Description	Type	Size
aaa-shared-secret	AAA shared secret.	password	Not Specified
access-point-name	Access point name(APN).	string	Maximum length: 63
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.	
at-dial-script	Initialization AT commands specific to the MODEM.	string	Maximum length: 127
billing-start-day	Billing start day.	integer	Minimum value: 1 Maximum value: 28
cdma-aaa-spi	CDMA AAA SPI.	string	Maximum length: 31
cdma-ha-spi	CDMA HA SPI.	string	Maximum length: 31
cdma-nai	NAI for CDMA MODEMS.	string	Maximum length: 31
conn-status	Connection status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
description	Description.	string	Maximum length: 31
dial-mode	Dial mode (dial-on-demand or always-connect).	option	-
	Option	Description	
	dial-on-demand	The dial action is controlled by user.	

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>always-connect</i></td><td>auto dial.</td></tr></table>			Option	Description	<i>always-connect</i>	auto dial.				
	Option	Description									
<i>always-connect</i>	auto dial.										
dial-status	Dial status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
ext-name	FortiExtender name.	string	Maximum length: 31								
ha-shared-secret	HA shared secret.	password	Not Specified								
id	FortiExtender serial number.	string	Maximum length: 19								
ifname	FortiExtender interface name.	string	Maximum length: 15								
initiated-update	Allow/disallow network initiated updates to the MODEM.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable network_initiated_update option.</td></tr><tr><td><i>disable</i></td><td>Disable network_initiated_update option.</td></tr></table>			Option	Description	<i>enable</i>	Enable network_initiated_update option.	<i>disable</i>	Disable network_initiated_update option.		
	Option	Description									
	<i>enable</i>	Enable network_initiated_update option.									
<i>disable</i>	Disable network_initiated_update option.										
mode	FortiExtender mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone.</td></tr><tr><td><i>redundant</i></td><td>Redundant for an interface.</td></tr></table>			Option	Description	<i>standalone</i>	Standalone.	<i>redundant</i>	Redundant for an interface.		
	Option	Description									
	<i>standalone</i>	Standalone.									
<i>redundant</i>	Redundant for an interface.										
modem-passwd	MODEM password.	password	Not Specified								
modem-type	MODEM type (CDMA, GSM/LTE or WIMAX).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cdma</i></td><td>CDMA</td></tr><tr><td><i>gsm/lte</i></td><td>GSM/LTE</td></tr><tr><td><i>wimax</i></td><td>WIMAX</td></tr></table>			Option	Description	<i>cdma</i>	CDMA	<i>gsm/lte</i>	GSM/LTE	<i>wimax</i>	WIMAX
	Option	Description									
	<i>cdma</i>	CDMA									
	<i>gsm/lte</i>	GSM/LTE									
<i>wimax</i>	WIMAX										
multi-mode	MODEM mode of operation(3G,LTE,etc).	option	-								

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>AUTO</td></tr><tr><td><i>auto-3g</i></td><td>Auto 3G(3G or less)</td></tr><tr><td><i>force-lte</i></td><td>Force LTE</td></tr><tr><td><i>force-3g</i></td><td>Force 3G</td></tr><tr><td><i>force-2g</i></td><td>Force 2G</td></tr></table>	Option	Description	<i>auto</i>	AUTO	<i>auto-3g</i>	Auto 3G(3G or less)	<i>force-lte</i>	Force LTE	<i>force-3g</i>	Force 3G	<i>force-2g</i>	Force 2G		
	Option	Description													
	<i>auto</i>	AUTO													
	<i>auto-3g</i>	Auto 3G(3G or less)													
	<i>force-lte</i>	Force LTE													
	<i>force-3g</i>	Force 3G													
<i>force-2g</i>	Force 2G														
ppp-auth-protocol	PPP authentication protocol (PAP,CHAP or auto).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>AUTO</td></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr></table>	Option	Description	<i>auto</i>	AUTO	<i>pap</i>	PAP	<i>chap</i>	CHAP						
	Option	Description													
	<i>auto</i>	AUTO													
	<i>pap</i>	PAP													
<i>chap</i>	CHAP														
ppp-echo-request	Enable/disable PPP echo request.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PPP echo request option.</td></tr><tr><td><i>disable</i></td><td>Disable PPP echo request option.</td></tr></table>	Option	Description	<i>enable</i>	Enable PPP echo request option.	<i>disable</i>	Disable PPP echo request option.								
	Option	Description													
	<i>enable</i>	Enable PPP echo request option.													
<i>disable</i>	Disable PPP echo request option.														
ppp-password	PPP password.	password	Not Specified												
ppp-username	PPP username.	string	Maximum length: 31												
primary-ha	Primary HA.	string	Maximum length: 31												
quota-limit-mb	Monthly quota limit (MB).	integer	Minimum value: 0 Maximum value: 10485760												
redial	Number of redials allowed based on failed attempts.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Forever.</td></tr><tr><td><i>1</i></td><td>One attempt.</td></tr></table>	Option	Description	<i>none</i>	Forever.	<i>1</i>	One attempt.								
	Option	Description													
	<i>none</i>	Forever.													
<i>1</i>	One attempt.														

Parameter	Description	Type	Size																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2</td><td>Two attempts.</td></tr><tr><td>3</td><td>Three attempts.</td></tr><tr><td>4</td><td>Four attempts.</td></tr><tr><td>5</td><td>Five attempts.</td></tr><tr><td>6</td><td>Six attempts.</td></tr><tr><td>7</td><td>Seven attempts.</td></tr><tr><td>8</td><td>Eight attempts.</td></tr><tr><td>9</td><td>Nine attempts.</td></tr><tr><td>10</td><td>Ten attempts.</td></tr></table>	Option	Description	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.		
	Option	Description																					
	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																				
roaming	Enable/disable MODEM roaming.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable GSM/LTE roaming option.</td></tr><tr><td>disable</td><td>Disable GSM/LTE roaming option.</td></tr></table>	Option	Description	enable	Enable GSM/LTE roaming option.	disable	Disable GSM/LTE roaming option.																
	Option	Description																					
	enable	Enable GSM/LTE roaming option.																					
disable	Disable GSM/LTE roaming option.																						
role	FortiExtender work role(Primary, Secondary, None).	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>FortiExtender is not supplying any service.</td></tr><tr><td>primary</td><td>FortiExtender is supplying primary service.</td></tr><tr><td>secondary</td><td>FortiExtender is standby for primary FortiExtender.</td></tr></table>	Option	Description	none	FortiExtender is not supplying any service.	primary	FortiExtender is supplying primary service.	secondary	FortiExtender is standby for primary FortiExtender.														
	Option	Description																					
	none	FortiExtender is not supplying any service.																					
	primary	FortiExtender is supplying primary service.																					
secondary	FortiExtender is standby for primary FortiExtender.																						
secondary-ha	Secondary HA.	string	Maximum length: 31																				
sim-pin	SIM PIN.	password	Not Specified																				
vdom	VDOM Read-only.	integer	Minimum value: 0 Maximum value: 4294967295																				
wimax-auth-protocol	WiMax authentication protocol(TLS or TTLS).	option	-																				

Parameter	Description	Type	Size
	Option	Description	
	<i>tls</i>	TLS	
	<i>ttls</i>	TTLS	
wimax-carrier	WiMax carrier.	string	Maximum length: 31
wimax-realm	WiMax realm.	string	Maximum length: 31

firewall

This section includes syntax for the following commands:

- [config firewall DoS-policy on page 142](#)
- [config firewall DoS-policy6 on page 144](#)
- [config firewall acl on page 147](#)
- [config firewall acl6 on page 148](#)
- [config firewall address on page 149](#)
- [config firewall address6-template on page 157](#)
- [config firewall address6 on page 154](#)
- [config firewall addrgrp on page 159](#)
- [config firewall addrgrp6 on page 160](#)
- [config firewall auth-portal on page 161](#)
- [config firewall central-snat-map on page 162](#)
- [config firewall consolidated policy on page 164](#)
- [config firewall dnstranslation on page 174](#)
- [config firewall identity-based-route on page 175](#)
- [config firewall interface-policy on page 176](#)
- [config firewall interface-policy6 on page 179](#)
- [config firewall internet-service-addition on page 184](#)
- [config firewall internet-service-append on page 186](#)
- [config firewall internet-service-custom-group on page 188](#)
- [config firewall internet-service-custom on page 186](#)
- [config firewall internet-service-definition on page 188](#)
- [config firewall internet-service-extension on page 190](#)
- [config firewall internet-service-group on page 193](#)
- [config firewall internet-service-ipbl-reason on page 194](#)
- [config firewall internet-service-ipbl-vendor on page 194](#)
- [config firewall internet-service-list on page 195](#)
- [config firewall internet-service-owner on page 195](#)
- [config firewall internet-service-reputation on page 196](#)
- [config firewall internet-service-sld on page 196](#)
- [config firewall internet-service on page 182](#)
- [config firewall ip-translation on page 202](#)
- [config firewall ipmacbinding setting on page 197](#)
- [config firewall ipmacbinding table on page 197](#)
- [config firewall ippool on page 198](#)
- [config firewall ippool6 on page 200](#)
- [config firewall ipv6-eh-filter on page 201](#)

-
- [config firewall ldb-monitor on page 203](#)
 - [config firewall local-in-policy on page 205](#)
 - [config firewall local-in-policy6 on page 206](#)
 - [config firewall multicast-address on page 207](#)
 - [config firewall multicast-address6 on page 209](#)
 - [config firewall multicast-policy on page 210](#)
 - [config firewall multicast-policy6 on page 212](#)
 - [config firewall policy on page 214](#)
 - [config firewall policy46 on page 233](#)
 - [config firewall policy6 on page 235](#)
 - [config firewall policy64 on page 246](#)
 - [config firewall profile-group on page 249](#)
 - [config firewall profile-protocol-options on page 250](#)
 - [config firewall proxy-address on page 269](#)
 - [config firewall proxy-addrgrp on page 273](#)
 - [config firewall proxy-policy on page 274](#)
 - [config firewall schedule group on page 281](#)
 - [config firewall schedule onetime on page 282](#)
 - [config firewall schedule recurring on page 282](#)
 - [config firewall security-policy on page 283](#)
 - [config firewall service category on page 290](#)
 - [config firewall service custom on page 290](#)
 - [config firewall service group on page 294](#)
 - [config firewall shaper per-ip-shaper on page 295](#)
 - [config firewall shaper traffic-shaper on page 296](#)
 - [config firewall shaping-policy on page 299](#)
 - [config firewall shaping-profile on page 303](#)
 - [config firewall sniffer on page 306](#)
 - [config firewall ssh host-key on page 311](#)
 - [config firewall ssh local-ca on page 312](#)
 - [config firewall ssh local-key on page 313](#)
 - [config firewall ssh setting on page 314](#)
 - [config firewall ssl-server on page 317](#)
 - [config firewall ssl-ssh-profile on page 320](#)
 - [config firewall ssl setting on page 315](#)
 - [config firewall traffic-class on page 335](#)
 - [config firewall ttl-policy on page 336](#)
 - [config firewall vip on page 337](#)
 - [config firewall vip46 on page 366](#)
 - [config firewall vip6 on page 369](#)
 - [config firewall vip64 on page 397](#)
 - [config firewall vipgrp on page 400](#)
 - [config firewall vipgrp46 on page 401](#)

- [config firewall vipgrp6 on page 402](#)
- [config firewall vipgrp64 on page 403](#)
- [config firewall wildcard-fqdn custom on page 403](#)
- [config firewall wildcard-fqdn group on page 404](#)

config firewall DoS-policy

Configure IPv4 DoS policies.

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

config firewall DoS-policy

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

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

config anomaly

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.	
log	Enable/disable anomaly logging.	option	-
	Option	Description	
	enable	Enable anomaly logging.	
	disable	Disable anomaly logging.	
name	Anomaly name.	string	Maximum length: 63
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. (Format ####d##h##m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-
	Option	Description	
	<i>disable</i>	Disable quarantine logging.	
	<i>enable</i>	Enable quarantine logging.	
status	Enable/disable this anomaly.	option	-
	Option	Description	
	<i>disable</i>	Disable this status.	
	<i>enable</i>	Enable this status.	
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 (1 - 2147483647, default = 1000). Note that each anomaly has a different threshold value assigned to it. Read-only.	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>
    config anomaly
      Description: Anomaly name.
      edit <name>
        set action [pass|block]
        set log [enable|disable]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set status [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
```



```

    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set interface {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
next
end

```

config firewall DoS-policy6

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

Option	Description
<i>enable</i>	Enable this policy.
<i>disable</i>	Disable this policy.

config anomaly

Parameter	Description	Type	Size
action	Action taken when the threshold is reached.	option	-

Option	Description
<i>pass</i>	Allow traffic but record a log message if logging is enabled.
<i>block</i>	Block traffic if this anomaly is found.

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

config firewall acl



This command is available for model(s): FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E.

It is not available for: FortiGate 1000D, FortiGate 200E, FortiGate 201E, FortiGate 300D, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 400D, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv4 access control list.

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

config firewall acl

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 1023
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79

Parameter	Description	Type	Size
interface	Interface name.	string	Maximum length: 35
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999
service <name>	Service name. Address name.	string	Maximum length: 79
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79
status	Enable/disable access control list status.	option	-

Option	Description
<i>enable</i>	Enable access control list status.
<i>disable</i>	Disable access control list status.

config firewall acl6



This command is available for model(s): FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E.

It is not available for: FortiGate 1000D, FortiGate 200E, FortiGate 201E, FortiGate 300D, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 400D, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv6 access control list.

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

config firewall acl6

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 1023
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79
interface	Interface name.	string	Maximum length: 35
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999
service <name>	Service name. Address name.	string	Maximum length: 79
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79
status	Enable/disable access control list status.	option	-

Option	Description
<i>enable</i>	Enable access control list status.
<i>disable</i>	Disable access control list status.

config firewall address

Configure IPv4 addresses.

```
config firewall address
    Description: Configure IPv4 addresses.
    edit <name>
```

```

set allow-routing [enable|disable]
set associated-interface {string}
set cache-ttl {integer}
set clearpass-spt [unknown|healthy|...]
set color {integer}
set comment {var-string}
set country {string}
set end-ip {ipv4-address-any}
set end-mac {mac-address}
set epg-name {string}
set filter {var-string}
set fqdn {string}
set fsso-group <name1>, <name2>, ...
set interface {string}
config list
    Description: IP address list.
    edit <ip>
    next
end
set obj-id {var-string}
set organization {string}
set policy-group {string}
set sdn {string}
set sdn-addr-type [private|public|...]
set sdn-tag {string}
set start-ip {ipv4-address-any}
set start-mac {mac-address}
set sub-type [sdn|clearpass-spt|...]
set subnet {ipv4-classnet-any}
set subnet-name {string}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set tenant {string}
set type [ipmask|iprange|...]
set uuid {uuid}
set visibility [enable|disable]
set wildcard {ipv4-classnet-any}
set wildcard-fqdn {string}
next
end

```

config firewall address

Parameter	Description	Type	Size
allow-routing	Enable/disable use of this address in the static route configuration.	option	-

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of this address in the static route configuration.</td></tr><tr><td><i>disable</i></td><td>Disable use of this address in the static route configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of this address in the static route configuration.	<i>disable</i>	Disable use of this address in the static route configuration.										
	Option	Description															
	<i>enable</i>	Enable use of this address in the static route configuration.															
<i>disable</i>	Disable use of this address in the static route configuration.																
associated-interface	Network interface associated with address.	string	Maximum length: 35														
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400														
clearpass-spt	SPT (System Posture Token) value.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unknown</i></td><td>UNKNOWN.</td></tr><tr><td><i>healthy</i></td><td>HEALTHY.</td></tr><tr><td><i>quarantine</i></td><td>QUARANTINE.</td></tr><tr><td><i>checkup</i></td><td>CHECKUP.</td></tr><tr><td><i>transient</i></td><td>TRANSIENT.</td></tr><tr><td><i>infected</i></td><td>INFECTED.</td></tr></table>	Option	Description	<i>unknown</i>	UNKNOWN.	<i>healthy</i>	HEALTHY.	<i>quarantine</i>	QUARANTINE.	<i>checkup</i>	CHECKUP.	<i>transient</i>	TRANSIENT.	<i>infected</i>	INFECTED.		
	Option	Description															
	<i>unknown</i>	UNKNOWN.															
	<i>healthy</i>	HEALTHY.															
	<i>quarantine</i>	QUARANTINE.															
	<i>checkup</i>	CHECKUP.															
	<i>transient</i>	TRANSIENT.															
<i>infected</i>	INFECTED.																
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32														
comment	Comment.	var-string	Maximum length: 255														
country	IP addresses associated to a specific country.	string	Maximum length: 2														
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified														
end-mac	Last MAC address in the range.	mac-address	Not Specified														
epg-name	Endpoint group name.	string	Maximum length: 255														
filter	Match criteria filter.	var-string	Maximum length: 2047														

Parameter	Description	Type	Size
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255
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
name	Address name.	string	Maximum length: 79
obj-id	Object ID for NSX.	var-string	Maximum length: 255
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35
policy-group	Policy group name.	string	Maximum length: 15
sdn	SDN.	string	Maximum length: 35
sdn-addr-type	Type of addresses to collect.	option	-

Option	Description
<i>private</i>	Collect private addresses only.
<i>public</i>	Collect public addresses only.
<i>all</i>	Collect both public and private addresses.

sdn-tag	SDN Tag.	string	Maximum length: 15
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified
start-mac	First MAC address in the range.	mac-address	Not Specified
sub-type	Sub-type of address.	option	-

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

Parameter	Description	Type	Size
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified
subnet-name	Subnet name.	string	Maximum length: 255
tenant	Tenant.	string	Maximum length: 35
type	Type of address.	option	-

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

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

Option	Description
<i>enable</i>	Show in address4 selection.
<i>disable</i>	Hide from address4 selection.

wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255

config list

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

config tagging

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

config firewall address6

Configure IPv6 firewall addresses.

```
config firewall address6
  Description: Configure IPv6 firewall addresses.
  edit <name>
    set cache-ttl {integer}
    set color {integer}
    set comment {var-string}
    set end-ip {ipv6-address}
    set end-mac {mac-address}
    set fqdn {string}
    set host {ipv6-address}
    set host-type [any|specific]
    set ip6 {ipv6-network}
    config list
      Description: IP address list.
      edit <ip>
        next
      end
    set obj-id {var-string}
    set sdn {string}
    set start-ip {ipv6-address}
    set start-mac {mac-address}
    config subnet-segment
      Description: IPv6 subnet segments.
      edit <name>
        set type [any|specific]
        set value {string}
      next
    end
    config tagging
      Description: Config object tagging
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set template {string}
    set type [ipprefix|iprange|...]
```

```

        set uuid {uuid}
        set visibility [enable|disable]
    next
end

```

config firewall address6

Parameter	Description	Type	Size						
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400						
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32						
comment	Comment.	var-string	Maximum length: 255						
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						
end-mac	Last MAC address in the range.	mac-address	Not Specified						
fqdn	Fully qualified domain name.	string	Maximum length: 255						
host	Host Address.	ipv6-address	Not Specified						
host-type	Host type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Wildcard.</td></tr><tr><td><i>specific</i></td><td>Specific host address.</td></tr></table>			Option	Description	<i>any</i>	Wildcard.	<i>specific</i>	Specific host address.
	Option	Description							
	<i>any</i>	Wildcard.							
<i>specific</i>	Specific host address.								
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified						
name	Address name.	string	Maximum length: 79						
obj-id	Object ID for NSX.	var-string	Maximum length: 255						
sdn	SDN.	string	Maximum length: 35						

Parameter	Description	Type	Size
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
start-mac	First MAC address in the range.	mac-address	Not Specified
template	IPv6 address template.	string	Maximum length: 63
type	Type of IPv6 address object (default = ipprefix).	option	-

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

uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable the visibility of the object in the GUI.	option	-

Option	Description
<i>enable</i>	Show in address6 selection.
<i>disable</i>	Hide from address6 selection.

config list

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

config subnet-segment

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 63
type	Subnet segment type.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>any</i>	Wildcard.	
	<i>specific</i>	Specific subnet segment address.	
value	Subnet segment value.	string	Maximum length: 35

config tagging

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

config firewall address6-template

Configure IPv6 address templates.

```

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

```

config firewall address6-template

Parameter	Description	Type	Size
ip6	IPv6 address prefix.	ipv6-network	Not Specified
name	IPv6 address template name.	string	Maximum length: 63
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6

config subnet-segment

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

config values

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

config firewall addrgrp

Configure IPv4 address groups.

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

config firewall addrgrp

Parameter	Description	Type	Size
allow-routing	Enable/disable use of this group in the static route configuration.	option	-
	Option		Description
	<i>enable</i>		Enable use of this group in the static route configuration.
	<i>disable</i>		Disable use of this group in the static route configuration.
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
exclude	Enable/disable address exclusion.	option	-
	Option		Description
	<i>enable</i>		Enable address exclusion.
	<i>disable</i>		Disable address exclusion.

Parameter	Description	Type	Size
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79
name	Address group name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable address visibility in the GUI.	option	-

Option	Description
<i>enable</i>	Show in address group selection.
<i>disable</i>	Hide from address group selection.

config tagging

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

config firewall addrgrp6

Configure IPv6 address groups.

```
config firewall addrgrp6
  Description: Configure IPv6 address groups.
  edit <name>
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
```



```

        set uuid {uuid}
        set visibility [enable|disable]
    next
end

```

config firewall addrgrp6

Parameter	Description	Type	Size
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79
name	IPv6 address group name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable address group6 visibility in the GUI.	option	-

Option	Description
<i>enable</i>	Show in address group selection.
<i>disable</i>	Hide from address group selection.

config tagging

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

config firewall auth-portal

Configure firewall authentication portals.

```

config firewall auth-portal
    Description: Configure firewall authentication portals.
    set groups <name1>, <name2>, ...
    set identity-based-route {string}
    set portal-addr {string}
    set portal-addr6 {string}
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
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35
portal-addr	Address (or FQDN) of the authentication portal.	string	Maximum length: 63
portal-addr6	IPv6 address (or FQDN) of authentication portal.	string	Maximum length: 63

config firewall central-snat-map

Configure central SNAT policies.

```

config firewall central-snat-map
    Description: Configure central SNAT policies.
    edit <policyid>
        set comments {var-string}
        set dst-addr <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set nat [disable|enable]
        set nat-ippool <name1>, <name2>, ...
        set nat-port {user}
        set orig-addr <name1>, <name2>, ...
        set orig-port {user}
        set protocol {integer}
        set srcintf <name1>, <name2>, ...
        set status [enable|disable]
    next
end

```

config firewall central-snat-map

Parameter	Description	Type	Size						
comments	Comment.	var-string	Maximum length: 1023						
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	Enable/disable source NAT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable source NAT.</td></tr><tr><td>enable</td><td>Enable source NAT.</td></tr></table>	Option	Description	disable	Disable source NAT.	enable	Enable source NAT.		
Option	Description								
disable	Disable source NAT.								
enable	Enable source NAT.								
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79						
nat-port	Translated port or port range (0 to 65535).	user	Not Specified						
orig-addr <name>	Original address. Address name.	string	Maximum length: 79						
orig-port	Original TCP port (0 to 65535).	user	Not Specified						
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295						
protocol	Integer value for the protocol type (0 - 255).	integer	Minimum value: 0 Maximum value: 255						
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79						
status	Enable/disable the active status of this policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this policy.</td></tr><tr><td>disable</td><td>Disable this policy.</td></tr></table>	Option	Description	enable	Enable this policy.	disable	Disable this policy.		
Option	Description								
enable	Enable this policy.								
disable	Disable this policy.								

config firewall consolidated policy

Configure consolidated IPv4/IPv6 policies.

```
config firewall consolidated policy
  Description: Configure consolidated IPv4/IPv6 policies.
  edit <policyid>
    set action [accept|deny|...]
    set application-list {string}
    set auto-asic-offload [enable|disable]
    set av-profile {string}
    set captive-portal-exempt [enable|disable]
    set cifs-profile {string}
    set comments {var-string}
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set dlp-sensor {string}
    set dnsfilter-profile {string}
    set dstaddr-negate [enable|disable]
    set dstaddr4 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set emailfilter-profile {string}
    set fixedport [enable|disable]
    set fsso-groups <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    set http-policy-redirect [enable|disable]
    set icap-profile {string}
    set inbound [enable|disable]
    set inspection-mode [proxy|flow]
    set internet-service [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-id <id1>, <id2>, ...
    set internet-service-negate [enable|disable]
    set internet-service-src [enable|disable]
    set internet-service-src-custom <name1>, <name2>, ...
    set internet-service-src-custom-group <name1>, <name2>, ...
    set internet-service-src-group <name1>, <name2>, ...
    set internet-service-src-id <id1>, <id2>, ...
    set internet-service-src-negate [enable|disable]
    set ippool [enable|disable]
    set ips-sensor {string}
    set logtraffic [all|utm|...]
    set logtraffic-start [enable|disable]
    set name {string}
    set nat [enable|disable]
    set outbound [enable|disable]
    set per-ip-shaper {string}
    set poolname4 <name1>, <name2>, ...
    set poolname6 <name1>, <name2>, ...
    set profile-group {string}
```

```

set profile-protocol-options {string}
set profile-type [single|group]
set schedule {string}
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {integer}
set srcaddr-negate [enable|disable]
set srcaddr4 <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-ssh-profile {string}
set status [enable|disable]
set tcp-mss-receiver {integer}
set tcp-mss-sender {integer}
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set voip-profile {string}
set vpntunnel {string}
set waf-profile {string}
set wanopt [enable|disable]
set wanopt-detection [active|passive|...]
set wanopt-passive-opt [default|transparent|...]
set wanopt-peer {string}
set wanopt-profile {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}

```

next

end

config firewall consolidated policy

Parameter	Description	Type	Size
action	Policy action (allow/deny/ipsec).	option	-
	Option	Description	
	<i>accept</i>	Allows session that match the firewall policy.	
	<i>deny</i>	Blocks sessions that match the firewall policy.	
	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.	
application-list	Name of an existing Application list.	string	Maximum length: 35

Parameter	Description	Type	Size						
auto-asic-offload *	Enable/disable policy traffic ASIC offloading.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto ASIC offloading.</td></tr><tr><td><i>disable</i></td><td>Disable ASIC offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.		
Option	Description								
<i>enable</i>	Enable auto ASIC offloading.								
<i>disable</i>	Disable ASIC offloading.								
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35						
captive-portal-exempt	Enable exemption of some users from the captive portal.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exemption of captive portal.</td></tr><tr><td><i>disable</i></td><td>Disable exemption of captive portal.</td></tr></table>	Option	Description	<i>enable</i>	Enable exemption of captive portal.	<i>disable</i>	Disable exemption of captive portal.		
Option	Description								
<i>enable</i>	Enable exemption of captive portal.								
<i>disable</i>	Disable exemption of captive portal.								
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35						
comments	Comment.	var-string	Maximum length: 1023						
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward (original) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable forward (original) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward (original) traffic DiffServ.	<i>disable</i>	Disable forward (original) traffic DiffServ.		
Option	Description								
<i>enable</i>	Enable forward (original) traffic DiffServ.								
<i>disable</i>	Disable forward (original) traffic DiffServ.								
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reverse (reply) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable reverse (reply) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable reverse (reply) traffic DiffServ.	<i>disable</i>	Disable reverse (reply) traffic DiffServ.		
Option	Description								
<i>enable</i>	Enable reverse (reply) traffic DiffServ.								
<i>disable</i>	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						
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35						

Parameter	Description	Type	Size						
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35						
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable destination address negate.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable destination address negate.	<i>disable</i>	Disable destination address negate.		
Option	Description								
<i>enable</i>	Enable destination address negate.								
<i>disable</i>	Disable destination address negate.								
dstaddr4 <name>	Destination IPv4 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						
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79						
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35						
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511						
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79						
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP(S) policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP(S) policy redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP(S) policy redirect.	<i>disable</i>	Disable HTTP(S) policy redirect.		
Option	Description								
<i>enable</i>	Enable HTTP(S) policy redirect.								
<i>disable</i>	Disable HTTP(S) policy redirect.								

Parameter	Description	Type	Size						
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35						
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>proxy</i></td><td>Proxy based inspection.</td></tr><tr><td><i>flow</i></td><td>Flow based inspection.</td></tr></table>	Option	Description	<i>proxy</i>	Proxy based inspection.	<i>flow</i>	Flow based inspection.		
Option	Description								
<i>proxy</i>	Proxy based inspection.								
<i>flow</i>	Flow based inspection.								
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.		
Option	Description								
<i>enable</i>	Enable use of Internet Services in policy.								
<i>disable</i>	Disable use of Internet Services in policy.								
internet-service-custom<name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79						
internet-service-custom-group<name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79						
internet-service-group<name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79						
internet-service-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	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.		
	Option	Description							
	<i>enable</i>	Enable negated Internet Service match.							
<i>disable</i>	Disable negated Internet Service match.								
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services source in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services source in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.		
	Option	Description							
	<i>enable</i>	Enable use of Internet Services source in policy.							
<i>disable</i>	Disable use of Internet Services source in policy.								
internet-service-src-custom<name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79						
internet-service-src-custom-group<name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79						
internet-service-src-group<name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79						
internet-service-src-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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service source match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service source match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated Internet Service source match.	<i>disable</i>	Disable negated Internet Service source match.		
	Option	Description							
	<i>enable</i>	Enable negated Internet Service source match.							
<i>disable</i>	Disable negated Internet Service source match.								
ippool	Enable to use IP Pools for source NAT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size								
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35								
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
Option	Description										
<i>all</i>	Log all sessions accepted or denied by this policy.										
<i>utm</i>	Log traffic that has a security profile applied to it.										
<i>disable</i>	Disable all logging for this policy.										
logtraffic-start	Record logs when a session starts.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
name	Policy name.	string	Maximum length: 35								
nat	Enable/disable source NAT.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35								
policyid	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294								
poolname4 <name>	IPv4 pool names. IPv4 pool name.	string	Maximum length: 79								

Parameter	Description	Type	Size						
poolname6 <name>	IPv6 pool names. IPv6 pool name.	string	Maximum length: 79						
profile-group	Name of profile group.	string	Maximum length: 35						
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.		
Option	Description								
<i>single</i>	Do not allow security profile groups.								
<i>group</i>	Allow security profile groups.								
schedule	Schedule name.	string	Maximum length: 35						
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.		
Option	Description								
<i>enable</i>	Enable negated service match.								
<i>disable</i>	Disable negated service match.								
session-ttl	TTL in seconds for sessions accepted by this policy (0 means use the system default session TTL).	integer	Minimum value: 300 Maximum value: 2764800						
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable source address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.		
Option	Description								
<i>enable</i>	Enable source address negate.								
<i>disable</i>	Disable source address negate.								
srcaddr4 <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79						

Parameter	Description	Type	Size						
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79						
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79						
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35						
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SSH policy redirect.</td></tr><tr><td>disable</td><td>Disable SSH policy redirect.</td></tr></table>	Option	Description	enable	Enable SSH policy redirect.	disable	Disable SSH policy redirect.		
Option	Description								
enable	Enable SSH policy redirect.								
disable	Disable SSH policy redirect.								
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35						
status	Enable or disable this policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535						
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535						
traffic-shaper	Traffic shaper.	string	Maximum length: 35						
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35						
users <name>	Names of individual users that can authenticate with this policy. User 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	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35
wanopt *	Enable/disable WAN optimization.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
wanopt-detection *	WAN optimization auto-detection mode.	option	-
	Option	Description	
	<i>active</i>	Active WAN optimization peer auto-detection.	
	<i>passive</i>	Passive WAN optimization peer auto-detection.	
	<i>off</i>	Turn off WAN optimization peer auto-detection.	
wanopt-passive-opt *	WAN optimization passive mode options. This option decides what IP address will be used to connect to server.	option	-
	Option	Description	
	<i>default</i>	Allow client side WAN opt peer to decide.	
	<i>transparent</i>	Use address of client to connect to server.	
	<i>non-transparent</i>	Use local FortiGate address to connect to server.	
wanopt-peer *	WAN optimization peer.	string	Maximum length: 35
wanopt-profile *	WAN optimization profile.	string	Maximum length: 35

Parameter	Description	Type	Size
webcache *	Enable/disable web cache.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
webcache-https *	Enable/disable web cache for HTTPS.	option	-
	Option	Description	
	<i>disable</i>	Disable web cache for HTTPS.	
	<i>enable</i>	Enable web cache for HTTPS.	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63
webproxy-profile	Webproxy profile name.	string	Maximum length: 63

* This parameter may not exist in some models.

config firewall dnstranslation

Configure DNS translation.

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

config firewall dnstranslation

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified
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

config firewall identity-based-route

Configure identity based routing.

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

config firewall identity-based-route

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

config rule

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

config firewall interface-policy

Configure IPv4 interface policies.

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


config firewall interface-policy

Parameter	Description	Type	Size						
application-list	Application list name.	string	Maximum length: 35						
application-list-status	Enable/disable application control.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application control</td></tr><tr><td><i>disable</i></td><td>Disable application control</td></tr></table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control		
Option	Description								
<i>enable</i>	Enable application control								
<i>disable</i>	Disable application control								
av-profile	Antivirus profile.	string	Maximum length: 35						
av-profile-status	Enable/disable antivirus.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus</td></tr><tr><td><i>disable</i></td><td>Disable antivirus</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus		
Option	Description								
<i>enable</i>	Enable antivirus								
<i>disable</i>	Disable antivirus								
comments	Comments.	var-string	Maximum length: 1023						
dlp-sensor	DLP sensor name.	string	Maximum length: 35						
dlp-sensor-status	Enable/disable DLP.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
dsri	Enable/disable DSRI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSRI.</td></tr><tr><td><i>disable</i></td><td>Disable DSRI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.		
Option	Description								
<i>enable</i>	Enable DSRI.								
<i>disable</i>	Disable DSRI.								
dstaddr <name>	Address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79						

Parameter	Description	Type	Size								
emailfilter-profile	Email filter profile.	string	Maximum length: 35								
emailfilter-profile-status	Enable/disable email filter.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Email filter.</td></tr><tr><td><i>disable</i></td><td>Disable Email filter.</td></tr></table>	Option	Description	<i>enable</i>	Enable Email filter.	<i>disable</i>	Disable Email filter.				
Option	Description										
<i>enable</i>	Enable Email filter.										
<i>disable</i>	Disable Email filter.										
interface	Monitored interface name from available interfaces.	string	Maximum length: 35								
ips-sensor	IPS sensor name.	string	Maximum length: 35								
ips-sensor-status	Enable/disable IPS.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS.</td></tr><tr><td><i>disable</i></td><td>Disable IPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS.	<i>disable</i>	Disable IPS.				
Option	Description										
<i>enable</i>	Enable IPS.										
<i>disable</i>	Disable IPS.										
logtraffic	Logging type to be used in this policy (Options: all utm disable, Default: utm).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
Option	Description										
<i>all</i>	Log all sessions accepted or denied by this policy.										
<i>utm</i>	Log traffic that has a security profile applied to it.										
<i>disable</i>	Disable all logging for this policy.										
policyid	Policy ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295								
service <name>	Service object from available options. Service name.	string	Maximum length: 79								
srcaddr <name>	Address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79								
status	Enable/disable this policy.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable this policy.	
	<i>disable</i>	Disable this policy.	
webfilter-profile	Web filter profile.	string	Maximum length: 35
webfilter-profile-status	Enable/disable web filtering.	option	-
	Option	Description	
	<i>enable</i>	Enable web filtering.	
	<i>disable</i>	Disable web filtering.	

config firewall interface-policy6

Configure IPv6 interface policies.

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

config firewall interface-policy6

Parameter	Description	Type	Size						
application-list	Application list name.	string	Maximum length: 35						
application-list-status	Enable/disable application control.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application control</td></tr><tr><td><i>disable</i></td><td>Disable application control</td></tr></table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control		
Option	Description								
<i>enable</i>	Enable application control								
<i>disable</i>	Disable application control								
av-profile	Antivirus profile.	string	Maximum length: 35						
av-profile-status	Enable/disable antivirus.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus</td></tr><tr><td><i>disable</i></td><td>Disable antivirus</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus		
Option	Description								
<i>enable</i>	Enable antivirus								
<i>disable</i>	Disable antivirus								
comments	Comments.	var-string	Maximum length: 1023						
dlp-sensor	DLP sensor name.	string	Maximum length: 35						
dlp-sensor-status	Enable/disable DLP.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
dsri	Enable/disable DSRI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSRI.</td></tr><tr><td><i>disable</i></td><td>Disable DSRI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.		
Option	Description								
<i>enable</i>	Enable DSRI.								
<i>disable</i>	Disable DSRI.								
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						

Parameter	Description	Type	Size								
emailfilter-profile	Email filter profile.	string	Maximum length: 35								
emailfilter-profile-status	Enable/disable email filter.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Email filter.</td></tr><tr><td><i>disable</i></td><td>Disable Email filter.</td></tr></table>	Option	Description	<i>enable</i>	Enable Email filter.	<i>disable</i>	Disable Email filter.				
Option	Description										
<i>enable</i>	Enable Email filter.										
<i>disable</i>	Disable Email filter.										
interface	Monitored interface name from available interfaces.	string	Maximum length: 35								
ips-sensor	IPS sensor name.	string	Maximum length: 35								
ips-sensor-status	Enable/disable IPS.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS.</td></tr><tr><td><i>disable</i></td><td>Disable IPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS.	<i>disable</i>	Disable IPS.				
Option	Description										
<i>enable</i>	Enable IPS.										
<i>disable</i>	Disable IPS.										
logtraffic	Logging type to be used in this policy (Options: all utm disable, Default: utm).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
Option	Description										
<i>all</i>	Log all sessions accepted or denied by this policy.										
<i>utm</i>	Log traffic that has a security profile applied to it.										
<i>disable</i>	Disable all logging for this policy.										
policyid	Policy ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295								
service6 <name>	Service name. Address name.	string	Maximum length: 79								
srcaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79								
status	Enable/disable this policy.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable this policy.	
	<i>disable</i>	Disable this policy.	
webfilter-profile	Web filter profile.	string	Maximum length: 35
webfilter-profile-status	Enable/disable web filtering.	option	-
	Option	Description	
	<i>enable</i>	Enable web filtering.	
	<i>disable</i>	Disable web filtering.	

config firewall internet-service

Show Internet Service application. Read-only.

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

config firewall internet-service

Parameter	Description	Type	Size
database	Database name this Internet Service belongs to. Read-only.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>isdb</i></td><td>Internet Service Database.</td></tr><tr><td><i>irdb</i></td><td>Internet RRR Database.</td></tr></table>	Option	Description	<i>isdb</i>	Internet Service Database.	<i>irdb</i>	Internet RRR Database.				
	Option	Description									
	<i>isdb</i>	Internet Service Database.									
<i>irdb</i>	Internet RRR Database.										
direction	How this service may be used in a firewall policy (source, destination or both). Read-only.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>src</i></td><td>As source in the firewall policy.</td></tr><tr><td><i>dst</i></td><td>As destination in the firewall policy.</td></tr><tr><td><i>both</i></td><td>Both directions in the firewall policy.</td></tr></table>	Option	Description	<i>src</i>	As source in the firewall policy.	<i>dst</i>	As destination in the firewall policy.	<i>both</i>	Both directions in the firewall policy.		
	Option	Description									
	<i>src</i>	As source in the firewall policy.									
	<i>dst</i>	As destination in the firewall policy.									
<i>both</i>	Both directions in the firewall policy.										
extra-ip-range-number	Extra number of IP ranges. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
icon-id	Icon ID of Internet Service. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
id	Internet Service ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
ip-number	Total number of IP addresses. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
ip-range-number	Number of IP ranges. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
name	Internet Service name. Read-only.	string	Maximum length: 63								

Parameter	Description	Type	Size
obsolete	Indicates whether the Internet Service can be used. Read-only.	integer	Minimum value: 0 Maximum value: 255
reputation	Reputation level of the Internet Service. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
singularity	Singular level of the Internet Service. Read-only.	integer	Minimum value: 0 Maximum value: 65535
sld-id	Second Level Domain. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295

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

```


config firewall internet-service-addition

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

config entry

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

config port-range

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

config firewall internet-service-append

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

config firewall internet-service-custom

Configure custom Internet Services.

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

config firewall internet-service-custom

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

config entry

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

config port-range

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

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

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
name	Custom Internet Service group name.	string	Maximum length: 63

config firewall internet-service-definition

Configure Internet Service definition.

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

```

        next
      end
      set protocol {integer}
    next
  end
next
end

```

config firewall internet-service-definition

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

config entry

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

config port-range

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

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

config firewall internet-service-extension

Configure Internet Services Extension.

```
config firewall internet-service-extension
    Description: Configure Internet Services Extension.
    edit <id>
        set comment {var-string}
        config disable-entry
            Description: Disable entries in the Internet Service database.
            edit <id>
                config ip-range
                    Description: IP ranges in the disable entry.
                    edit <id>
                        set end-ip {ipv4-address-any}
                        set start-ip {ipv4-address-any}
                    next
                end
                config port-range
                    Description: Port ranges in the disable entry.
                    edit <id>
                        set end-port {integer}
                        set start-port {integer}
                    next
                end
                set protocol {integer}
            next
        end
    end
    config entry
        Description: Entries added to the Internet Service extension database.
        edit <id>
            set dst <name1>, <name2>, ...
            config port-range
                Description: Port ranges in the custom entry.
                edit <id>
                    set end-port {integer}
                    set start-port {integer}
                next
            end
            set protocol {integer}
        end
    end
end
```

```
        next
    end
next
end
```

config firewall internet-service-extension

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

config disable-entry

Parameter	Description	Type	Size
id	Disable entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	integer	Minimum value: 0 Maximum value: 255

config ip-range

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

config port-range

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

config entry

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

config port-range

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

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

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	
	<i>source</i>	As source when applied.	
	<i>destination</i>	As destination when applied.	
	<i>both</i>	Both directions when applied.	
member <id>	Internet Service group member. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Internet Service group name.	string	Maximum length: 63

config firewall internet-service-ipbl-reason

IP blacklist reason. Read-only.

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

config firewall internet-service-ipbl-reason

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

config firewall internet-service-ipbl-vendor

IP blacklist vendor. Read-only.

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

config firewall internet-service-ipbl-vendor

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

config firewall internet-service-list

Internet Service list. Read-only.

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

config firewall internet-service-list

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

config firewall internet-service-owner

Internet Service owner. Read-only.

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

config firewall internet-service-owner

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

config firewall internet-service-reputation

Show Internet Service reputation. Read-only.

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

config firewall internet-service-reputation

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

config firewall internet-service-sld

Internet Service Second Level Domain. Read-only.

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

config firewall internet-service-sld

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

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

config firewall ipmacbinding table

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

```
config firewall ipmacbinding table
    Description: Configure IP to MAC address pairs in the IP/MAC binding table.
    edit <seq-num>
```

```

        set ip {ipv4-address}
        set mac {mac-address}
        set name {string}
        set status [enable|disable]
    next
end

```

config firewall ipmacbinding table

Parameter	Description	Type	Size
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 hexadecimal).	mac-address	Not Specified
name	Name of the pair (optional, default = no name).	string	Maximum length: 35
seq-num	Entry number.	integer	Minimum value: 0 Maximum value: 4294967295
status	Enable/disable this IP-mac binding pair.	option	-

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

config firewall ippool

Configure IPv4 IP pools.

```

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

```

```

        set type [overload|one-to-one|...]
    next
end

```

config firewall ippool

Parameter	Description	Type	Size
arp-intf	Select an interface from available options that will reply to ARP requests. (If blank, any is selected).	string	Maximum length: 15
arp-reply	Enable/disable replying to ARP requests when an IP Pool is added to a policy (default = enable).	option	-
	Option	Description	
	disable	Disable ARP reply.	
	enable	Enable ARP reply.	
associated-interface	Associated interface name.	string	Maximum length: 15
block-size	Number of addresses in a block (64 to 4096, default = 128).	integer	Minimum value: 64 Maximum value: 4096
comments	Comment.	var-string	Maximum length: 255
endip	Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified
name	IP pool name.	string	Maximum length: 79
num-blocks-per-user	Number of addresses blocks that can be used by a user (1 to 128, default = 8).	integer	Minimum value: 1 Maximum value: 128
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.	

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

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

config firewall ippool6

Configure IPv6 IP pools.

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

config firewall ippool6

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 255
endip	Final IPv6 address (inclusive) in the range for the address pool (format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, Default: ::).	ipv6-address	Not Specified

Parameter	Description	Type	Size
name	IPv6 IP pool name.	string	Maximum length: 79
startip	First IPv6 address (inclusive) in the range for the address pool (format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, Default: ::).	ipv6-address	Not Specified

config firewall ipv6-eh-filter

Configure IPv6 extension header filter.

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

config firewall ipv6-eh-filter

Parameter	Description	Type	Size						
auth	Enable/disable blocking packets with the Authentication header (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with the Authentication header.</td></tr><tr><td><i>disable</i></td><td>Allow packets with the Authentication header.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with the Authentication header.	<i>disable</i>	Allow packets with the Authentication header.		
Option	Description								
<i>enable</i>	Block packets with the Authentication header.								
<i>disable</i>	Allow packets with the Authentication header.								
dest-opt	Enable/disable blocking packets with Destination Options headers (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking packets with Destination Options headers.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with Destination Options headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable blocking packets with Destination Options headers.	<i>disable</i>	Disable blocking packets with Destination Options headers.		
Option	Description								
<i>enable</i>	Enable blocking packets with Destination Options headers.								
<i>disable</i>	Disable blocking packets with Destination Options headers.								
fragment	Enable/disable blocking packets with the Fragment header (default = disable).	option	-						

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

config firewall ip-translation

Configure firewall IP-translation.

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

```

        set startip {ipv4-address-any}
        set type {option}
    next
end

```

config firewall ip-translation

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

Option	Description
SCTP	SCTP

config firewall ldb-monitor

Configure server load balancing health monitors.

```

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

```

config firewall ldb-monitor

Parameter	Description	Type	Size
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 (0 - 5, default = 0).	integer	Minimum value: 0 Maximum value: 5
interval	Time between health checks (5 - 65635 sec, default = 10).	integer	Minimum value: 5 Maximum value: 65535
name	Monitor name.	string	Maximum length: 35
port	Service port used to perform the health check. If 0, health check monitor inherits port configured for the server (0 - 65635, default = 0).	integer	Minimum value: 0 Maximum value: 65535
retry	Number health check attempts before the server is considered down (1 - 255, default = 3).	integer	Minimum value: 1 Maximum value: 255
timeout	Time to wait to receive response to a health check from a server. Reaching the timeout means the health check failed (1 - 255 sec, default = 2).	integer	Minimum value: 1 Maximum value: 255
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
<i>ping</i>	PING health monitor.
<i>tcp</i>	TCP-connect health monitor.
<i>http</i>	HTTP-GET health monitor.
<i>https</i>	HTTP-GET health monitor with SSL.

config firewall local-in-policy

Configure user defined IPv4 local-in policies.

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

config firewall local-in-policy

Parameter	Description	Type	Size
action	Action performed on traffic matching the policy (default = deny).	option	-
	Option		
	<i>accept</i>		
	<i>deny</i>		
comments	Comment.	var-string	Maximum length: 1023
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79
ha-mgmt-intf-only	Enable/disable dedicating the HA management interface only for local-in policy.	option	-
	Option		
	<i>enable</i>		
	<i>disable</i>		
intf	Incoming interface name from available options.	string	Maximum length: 35

Parameter	Description	Type	Size
policyid	User defined local in policy ID.	integer	Minimum value: 0 Maximum value: 4294967295
schedule	Schedule object from available options.	string	Maximum length: 35
service <name>	Service object from available options. Service name.	string	Maximum length: 79
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79
status	Enable/disable this local-in policy.	option	-

Option	Description
<i>enable</i>	Enable this local-in policy.
<i>disable</i>	Disable this local-in policy.

config firewall local-in-policy6

Configure user defined IPv6 local-in policies.

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

config firewall local-in-policy6

Parameter	Description	Type	Size
action	Action performed on traffic matching the policy (default = deny).	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.	
comments	Comment.	var-string	Maximum length: 1023
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79
intf	Incoming interface name from available options.	string	Maximum length: 35
policyid	User defined local in policy ID.	integer	Minimum value: 0 Maximum value: 4294967295
schedule	Schedule object from available options.	string	Maximum length: 35
service <name>	Service object from available options. Separate names with a space. Service name.	string	Maximum length: 79
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79
status	Enable/disable this local-in policy.	option	-
	Option	Description	
	enable	Enable this local-in policy.	
	disable	Disable this local-in policy.	

config firewall multicast-address

Configure multicast addresses.

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

```

config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set type [multicastrange|broadcastmask]
set visibility [enable|disable]
next
end

```

config firewall multicast-address

Parameter	Description	Type	Size						
associated-interface	Interface associated with the address object. When setting up a policy, only addresses associated with this interface are available.	string	Maximum length: 35						
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1).	integer	Minimum value: 0 Maximum value: 32						
comment	Comment.	var-string	Maximum length: 255						
end-ip	Final IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified						
name	Multicast address name.	string	Maximum length: 79						
start-ip	First IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified						
subnet	Broadcast address and subnet.	ipv4-classnet-any	Not Specified						
type	Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multicastrange</i></td><td>Multicast range.</td></tr><tr><td><i>broadcastmask</i></td><td>Broadcast IP/mask.</td></tr></table>			Option	Description	<i>multicastrange</i>	Multicast range.	<i>broadcastmask</i>	Broadcast IP/mask.
Option	Description								
<i>multicastrange</i>	Multicast range.								
<i>broadcastmask</i>	Broadcast IP/mask.								
visibility	Enable/disable visibility of the multicast address on the GUI.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Show the multicast address on the GUI.	
	<i>disable</i>	Hide the multicast address from the GUI.	

config tagging

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

config firewall multicast-address6

Configure IPv6 multicast address.

```

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

```

config firewall multicast-address6

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified
name	IPv6 multicast address name.	string	Maximum length: 79
visibility	Enable/disable visibility of the IPv6 multicast address on the GUI.	option	-
		Option	Description
		<i>enable</i>	Show the IPv6 multicast address on the GUI.
		<i>disable</i>	Hide the IPv6 multicast address from the GUI.

config tagging

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

config firewall multicast-policy

Configure multicast NAT policies.

```
config firewall multicast-policy
  Description: Configure multicast NAT policies.
  edit <id>
    set action [accept|deny]
    set auto-asic-offload [enable|disable]
    set dnat {ipv4-address-any}
    set dstaddr <name1>, <name2>, ...
    set dstintf {string}
```

```

    set end-port {integer}
    set logtraffic [enable|disable]
    set protocol {integer}
    set snat [enable|disable]
    set snat-ip {ipv4-address}
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set start-port {integer}
    set status [enable|disable]
next
end

```

config firewall multicast-policy

Parameter	Description	Type	Size
action	Accept or deny traffic matching the policy.	option	-
	Option	Description	
	<i>accept</i>	Accept traffic matching the policy.	
	<i>deny</i>	Deny or block traffic matching the policy.	
auto-asic-offload *	Enable/disable offloading policy traffic for hardware acceleration.	option	-
	Option	Description	
	<i>enable</i>	Enable hardware acceleration offloading.	
	<i>disable</i>	Disable offloading for hardware acceleration.	
dnat	IPv4 DNAT address used for multicast destination addresses.	ipv4-address-any	Not Specified
dstaddr <name>	Destination address objects. Destination address objects.	string	Maximum length: 79
dstintf	Destination interface name.	string	Maximum length: 35
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 - 65535, default = 1).	integer	Minimum value: 0 Maximum value: 65535
id	Policy ID ((0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable logging traffic accepted by this policy.	
	<i>disable</i>	Disable logging traffic accepted by this policy.	
protocol	Integer value for the protocol type as defined by IANA (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255
snat	Enable/disable substitution of the outgoing interface IP address for the original source IP address (called source NAT or SNAT).	option	-
	Option	Description	
	<i>enable</i>	Enable source NAT.	
	<i>disable</i>	Disable source NAT.	
snat-ip	IPv4 address to be used as the source address for NATed traffic.	ipv4-address	Not Specified
srcaddr <name>	Source address objects. Source address objects.	string	Maximum length: 79
srcintf	Source interface name.	string	Maximum length: 35
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 - 65535, default = 1).	integer	Minimum value: 0 Maximum value: 65535
status	Enable/disable this policy.	option	-
	Option	Description	
	<i>enable</i>	Enable this policy.	
	<i>disable</i>	Disable this policy.	

* This parameter may not exist in some models.

config firewall multicast-policy6

Configure IPv6 multicast NAT policies.

```
config firewall multicast-policy6
    Description: Configure IPv6 multicast NAT policies.
    edit <id>
```

```

    set action [accept|deny]
    set auto-asic-offload [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set dstintf {string}
    set end-port {integer}
    set logtraffic [enable|disable]
    set protocol {integer}
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set start-port {integer}
    set status [enable|disable]
next
end

```

config firewall multicast-policy6

Parameter	Description	Type	Size
action	Accept or deny traffic matching the policy.	option	-
	Option	Description	
	<i>accept</i>	Accept.	
	<i>deny</i>	Deny.	
auto-asic-offload *	Enable/disable offloading policy traffic for hardware acceleration.	option	-
	Option	Description	
	<i>enable</i>	Enable offloading policy traffic for hardware acceleration.	
	<i>disable</i>	Disable offloading policy traffic for hardware acceleration.	
dstaddr <name>	IPv6 destination address name. Address name.	string	Maximum length: 79
dstintf	IPv6 destination interface name.	string	Maximum length: 35
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (1 - 65535, default = 65535).	integer	Minimum value: 0 Maximum value: 65535
id	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging traffic accepted by this policy.</td></tr><tr><td><i>disable</i></td><td>Disable logging traffic accepted by this policy.</td></tr></table>			Option	Description	<i>enable</i>	Enable logging traffic accepted by this policy.	<i>disable</i>	Disable logging traffic accepted by this policy.
Option	Description								
<i>enable</i>	Enable logging traffic accepted by this policy.								
<i>disable</i>	Disable logging traffic accepted by this policy.								
protocol	Integer value for the protocol type as defined by IANA (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255						
srcaddr <name>	IPv6 source address name. Address name.	string	Maximum length: 79						
srcintf	IPv6 source interface name.	string	Maximum length: 35						
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (1 - 65535, default = 1).	integer	Minimum value: 0 Maximum value: 65535						
status	Enable/disable this policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>			Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.
Option	Description								
<i>enable</i>	Enable this policy.								
<i>disable</i>	Disable this policy.								

* This parameter may not exist in some models.

config firewall policy

Configure IPv4 policies.

```
config firewall policy
  Description: Configure IPv4 policies.
  edit <policyid>
    set action [accept|deny|...]
    set anti-replay [enable|disable]
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set application-list {string}
    set auth-cert {string}
    set auth-path [enable|disable]
    set auth-redirect-addr {string}
    set auto-asic-offload [enable|disable]
    set av-profile {string}
    set block-notification [enable|disable]
    set captive-portal-exempt [enable|disable]
```

```
set capture-packet [enable|disable]
set cifs-profile {string}
set comments {var-string}
set custom-log-fields <field-id1>, <field-id2>, ...
set delay-tcp-npu-session [enable|disable]
set diffserv-forward [enable|disable]
set diffserv-reverse [enable|disable]
set diffservcode-forward {user}
set diffservcode-rev {user}
set disclaimer [enable|disable]
set dlp-sensor {string}
set dnsfilter-profile {string}
set dsri [enable|disable]
set dstaddr <name1>, <name2>, ...
set dstaddr-negate [enable|disable]
set dstintf <name1>, <name2>, ...
set email-collect [enable|disable]
set emailfilter-profile {string}
set firewall-session-dirty [check-all|check-new]
set fixedport [enable|disable]
set fsso [enable|disable]
set fsso-agent-for-ntlm {string}
set fsso-groups <name1>, <name2>, ...
set geoip-anycast [enable|disable]
set groups <name1>, <name2>, ...
set http-policy-redirect [enable|disable]
set icap-profile {string}
set identity-based-route {string}
set inbound [enable|disable]
set inspection-mode [proxy|flow]
set internet-service [enable|disable]
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-id <id1>, <id2>, ...
set internet-service-negate [enable|disable]
set internet-service-src [enable|disable]
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-id <id1>, <id2>, ...
set internet-service-src-negate [enable|disable]
set ippool [enable|disable]
set ips-sensor {string}
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set match-vip [enable|disable]
set match-vip-only [enable|disable]
set name {string}
set nat [enable|disable]
set natinbound [enable|disable]
set natip {ipv4-classnet}
set natoutbound [enable|disable]
set np-acceleration [enable|disable]
set ntlm [enable|disable]
set ntlm-enabled-browsers <user-agent-string1>, <user-agent-string2>, ...
```

```
set ntlm-guest [enable|disable]
set outbound [enable|disable]
set per-ip-shaper {string}
set permit-any-host [enable|disable]
set permit-stun-host [enable|disable]
set poolname <name1>, <name2>, ...
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set radius-mac-auth-bypass [enable|disable]
set redirect-url {string}
set replacemsg-override-group {string}
set reputation-direction [source|destination]
set reputation-minimum {integer}
set rso [enable|disable]
set rtp-addr <name1>, <name2>, ...
set rtp-nat [disable|enable]
set schedule {string}
set schedule-timeout [enable|disable]
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {user}
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-mirror [enable|disable]
set ssl-mirror-intf <name1>, <name2>, ...
set ssl-ssh-profile {string}
set status [enable|disable]
set tcp-mss-receiver {integer}
set tcp-mss-sender {integer}
set tcp-session-without-syn [all|data-only|...]
set timeout-send-rst [enable|disable]
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set url-category <id1>, <id2>, ...
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set vlan-cos-fwd {integer}
set vlan-cos-rev {integer}
set vlan-filter {user}
set voip-profile {string}
set vptunnel {string}
set waf-profile {string}
set wanopt [enable|disable]
set wanopt-detection [active|passive|...]
set wanopt-passive-opt [default|transparent|...]
set wanopt-peer {string}
set wanopt-profile {string}
```



```

    set wccp [enable|disable]
    set webcache [enable|disable]
    set webcache-https [disable|enable]
    set webfilter-profile {string}
    set webproxy-forward-server {string}
    set webproxy-profile {string}
    set wso [enable|disable]
next
end

```

config firewall policy

Parameter	Description	Type	Size
action	Policy action (allow/deny/ipsec).	option	-
	Option	Description	
	<i>accept</i>	Allows session that match the firewall policy.	
	<i>deny</i>	Blocks sessions that match the firewall policy.	
	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.	
anti-replay	Enable/disable anti-replay check.	option	-
	Option	Description	
	<i>enable</i>	Enable anti-replay check.	
	<i>disable</i>	Disable anti-replay check.	
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295
app-group <name>	Application group names. Application group names.	string	Maximum length: 79
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295
application-list	Name of an existing Application list.	string	Maximum length: 35
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35
auth-path	Enable/disable authentication-based routing.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable authentication-based routing.	
	<i>disable</i>	Disable authentication-based routing.	
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication.	string	Maximum length: 63
auto-asic-offload *	Enable/disable policy traffic ASIC offloading.	option	-
	Option	Description	
	<i>enable</i>	Enable auto ASIC offloading.	
	<i>disable</i>	Disable ASIC offloading.	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
block-notification	Enable/disable block notification.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
captive-portal-exempt	Enable to exempt some users from the captive portal.	option	-
	Option	Description	
	<i>enable</i>	Enable exemption of captive portal.	
	<i>disable</i>	Disable exemption of captive portal.	
capture-packet *	Enable/disable capture packets.	option	-
	Option	Description	
	<i>enable</i>	Enable capture packets.	
	<i>disable</i>	Disable capture packets.	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35
comments	Comment.	var-string	Maximum length: 1023

Parameter	Description	Type	Size
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35
delay-tcp-npu-session	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-
	Option	Description	
	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order handshake.	
	<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order handshake.	
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-
	Option	Description	
	<i>enable</i>	Enable setting forward (original) traffic Diffserv.	
	<i>disable</i>	Disable setting forward (original) traffic Diffserv.	
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-
	Option	Description	
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	
	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.	
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified
disclaimer	Enable/disable user authentication disclaimer.	option	-
	Option	Description	
	<i>enable</i>	Enable user authentication disclaimer.	
	<i>disable</i>	Disable user authentication disclaimer.	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35

Parameter	Description	Type	Size
dsri	Enable DSRI to ignore HTTP server responses.	option	-
	Option	Description	
	<i>enable</i>	Enable DSRI.	
	<i>disable</i>	Disable DSRI.	
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-
	Option	Description	
	<i>enable</i>	Enable destination address negate.	
	<i>disable</i>	Disable destination address negate.	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79
email-collect	Enable/disable email collection.	option	-
	Option	Description	
	<i>enable</i>	Enable email collection.	
	<i>disable</i>	Disable email collection.	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-
	Option	Description	
	<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.	
	<i>check-new</i>	Continue to allow sessions already accepted by this policy.	
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size
fsso	Enable/disable Fortinet Single Sign-On.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511
geoip-anycast	Enable/disable recognition of anycast IP addresses using the geography IP database.	option	-
	Option	Description	
	<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.	
	<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.	
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-
	Option	Description	
	<i>enable</i>	Enable HTTP(S) policy redirect.	
	<i>disable</i>	Disable HTTP(S) policy redirect.	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35
identity-based-route	Name of identity-based routing rule.	string	Maximum length: 35
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size						
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>proxy</i></td><td>Proxy based inspection.</td></tr><tr><td><i>flow</i></td><td>Flow based inspection.</td></tr></table>	Option	Description	<i>proxy</i>	Proxy based inspection.	<i>flow</i>	Flow based inspection.		
Option	Description								
<i>proxy</i>	Proxy based inspection.								
<i>flow</i>	Flow based inspection.								
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.		
Option	Description								
<i>enable</i>	Enable use of Internet Services in policy.								
<i>disable</i>	Disable use of Internet Services in policy.								
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79						
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79						
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79						
internet-service-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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.		
Option	Description								
<i>enable</i>	Enable negated Internet Service match.								
<i>disable</i>	Disable negated Internet Service match.								
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	enable	Enable use of Internet Services source in policy.	
	disable	Disable use of Internet Services source in policy.	
internet-service-src-custom<name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79
internet-service-src-custom-group<name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79
internet-service-src-group<name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79
internet-service-src-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.	
ippool	Enable to use IP Pools for source NAT.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
	Option	Description									
	<i>all</i>	Log all sessions accepted or denied by this policy.									
	<i>utm</i>	Log traffic that has a security profile applied to it.									
<i>disable</i>	Disable all logging for this policy.										
logtraffic-start	Record logs when a session starts.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
match-vip	Enable to match packets that have had their destination addresses changed by a VIP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match DNATed packet.</td></tr><tr><td><i>disable</i></td><td>Do not match DNATed packet.</td></tr></table>	Option	Description	<i>enable</i>	Match DNATed packet.	<i>disable</i>	Do not match DNATed packet.				
	Option	Description									
	<i>enable</i>	Match DNATed packet.									
<i>disable</i>	Do not match DNATed packet.										
match-vip-only	Enable/disable matching of only those packets that have had their destination addresses changed by a VIP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable matching of only those packets that have had their destination addresses changed by a VIP.</td></tr><tr><td><i>disable</i></td><td>Disable matching of only those packets that have had their destination addresses changed by a VIP.</td></tr></table>	Option	Description	<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.	<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.				
	Option	Description									
	<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.									
<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.										
name	Policy name.	string	Maximum length: 35								
nat	Enable/disable source NAT.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
natip	Policy-based IPsec VPN: source NAT IP address for outgoing traffic.	ipv4-classnet	Not Specified
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
np-acceleration *	Enable/disable UTM Network Processor acceleration.	option	-
	Option	Description	
	<i>enable</i>	Enable UTM Network Processor acceleration.	
	<i>disable</i>	Disable UTM Network Processor acceleration.	
ntlm	Enable/disable NTLM authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
ntlm-enabled-browsers <user-agent-string>	HTTP-User-Agent value of supported browsers. User agent string.	string	Maximum length: 79
ntlm-guest	Enable/disable NTLM guest user access.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35						
permit-any-host	Accept UDP packets from any host.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
permit-stun-host	Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
policyid	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294						
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79						
profile-group	Name of profile group.	string	Maximum length: 35						
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.		
	Option	Description							
	<i>single</i>	Do not allow security profile groups.							
<i>group</i>	Allow security profile groups.								

Parameter	Description	Type	Size						
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC authentication bypass.</td></tr><tr><td><i>disable</i></td><td>Disable MAC authentication bypass.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC authentication bypass.	<i>disable</i>	Disable MAC authentication bypass.		
Option	Description								
<i>enable</i>	Enable MAC authentication bypass.								
<i>disable</i>	Disable MAC authentication bypass.								
redirect-url	URL users are directed to after seeing and accepting the disclaimer or authenticating.	string	Maximum length: 255						
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35						
reputation-direction	Direction of the initial traffic for reputation to take effect.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source</i></td><td>Check reputation for source address.</td></tr><tr><td><i>destination</i></td><td>Check reputation for destination address.</td></tr></table>	Option	Description	<i>source</i>	Check reputation for source address.	<i>destination</i>	Check reputation for destination address.		
Option	Description								
<i>source</i>	Check reputation for source address.								
<i>destination</i>	Check reputation for destination address.								
reputation-minimum	Minimum Reputation to take action.	integer	Minimum value: 0 Maximum value: 4294967295						
rsso	Enable/disable RADIUS single sign-on (RSSO).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
rtp-addr <name>	Address names if this is an RTP NAT policy. Address name.	string	Maximum length: 79						
rtp-nat	Enable Real Time Protocol (RTP) NAT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.	<i>enable</i>	Enable setting.		
Option	Description								
<i>disable</i>	Disable setting.								
<i>enable</i>	Enable setting.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable schedule timeout.</td></tr><tr><td><i>disable</i></td><td>Disable schedule timeout.</td></tr></table>	Option	Description	<i>enable</i>	Enable schedule timeout.	<i>disable</i>	Disable schedule timeout.		
Option	Description								
<i>enable</i>	Enable schedule timeout.								
<i>disable</i>	Disable schedule timeout.								
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable deny-packet sending.</td></tr><tr><td><i>enable</i></td><td>Enable deny-packet sending.</td></tr></table>	Option	Description	<i>disable</i>	Disable deny-packet sending.	<i>enable</i>	Enable deny-packet sending.		
Option	Description								
<i>disable</i>	Disable deny-packet sending.								
<i>enable</i>	Enable deny-packet sending.								
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79						
service-negate	When enabled service specifies what the service must NOT be.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.		
Option	Description								
<i>enable</i>	Enable negated service match.								
<i>disable</i>	Disable negated service match.								
session-ttl	TTL in seconds for sessions accepted by this policy (0 means use the system default session TTL).	user	Not Specified						
srcaddr <name>	Source address and address group names. Address name.	string	Maximum length: 79						
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable source address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.		
Option	Description								
<i>enable</i>	Enable source address negate.								
<i>disable</i>	Disable source address negate.								
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79						
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35						

Parameter	Description	Type	Size								
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable SSH policy redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH policy redirect.	<i>disable</i>	Disable SSH policy redirect.				
Option	Description										
<i>enable</i>	Enable SSH policy redirect.										
<i>disable</i>	Disable SSH policy redirect.										
ssl-mirror	Enable to copy decrypted SSL traffic to a FortiGate interface (called SSL mirroring).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL mirror.</td></tr><tr><td><i>disable</i></td><td>Disable SSL mirror.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL mirror.	<i>disable</i>	Disable SSL mirror.				
Option	Description										
<i>enable</i>	Enable SSL mirror.										
<i>disable</i>	Disable SSL mirror.										
ssl-mirror-intf <name>	SSL mirror interface name. Mirror Interface name.	string	Maximum length: 79								
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35								
status	Enable or disable this policy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535								
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535								
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Enable TCP session without SYN.</td></tr><tr><td><i>data-only</i></td><td>Enable TCP session data only.</td></tr><tr><td><i>disable</i></td><td>Disable TCP session without SYN.</td></tr></table>	Option	Description	<i>all</i>	Enable TCP session without SYN.	<i>data-only</i>	Enable TCP session data only.	<i>disable</i>	Disable TCP session without SYN.		
Option	Description										
<i>all</i>	Enable TCP session without SYN.										
<i>data-only</i>	Enable TCP session data only.										
<i>disable</i>	Disable TCP session without SYN.										

Parameter	Description	Type	Size
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-
	Option	Description	
	<i>enable</i>	Enable sending of RST packet upon TCP session expiration.	
	<i>disable</i>	Disable sending of RST packet upon TCP session expiration.	
tos	ToS (Type of Service) value used for comparison.	user	Not Specified
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	
	<i>enable</i>	Enable TOS match negate.	
	<i>disable</i>	Disable TOS match negate.	
traffic-shaper	Traffic shaper.	string	Maximum length: 35
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

Parameter	Description	Type	Size
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
vlan-filter	Set VLAN filters.	user	Not Specified
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35
wanopt *	Enable/disable WAN optimization.	option	-

Option	Description

<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

wanopt-detection *	WAN optimization auto-detection mode.	option	-

Option	Description

<i>active</i>	Active WAN optimization peer auto-detection.
<i>passive</i>	Passive WAN optimization peer auto-detection.
<i>off</i>	Turn off WAN optimization peer auto-detection.

wanopt-passive-opt *	WAN optimization passive mode options. This option decides what IP address will be used to connect server.	option	-

Option	Description

<i>default</i>	Allow client side WAN opt peer to decide.
<i>transparent</i>	Use address of client to connect to server.
<i>non-transparent</i>	Use local FortiGate address to connect to server.

Parameter	Description	Type	Size						
wanopt-peer *	WAN optimization peer.	string	Maximum length: 35						
wanopt-profile *	WAN optimization profile.	string	Maximum length: 35						
wccp	Enable/disable forwarding traffic matching this policy to a configured WCCP server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP setting.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable WCCP setting.	<i>disable</i>	Disable WCCP setting.		
Option	Description								
<i>enable</i>	Enable WCCP setting.								
<i>disable</i>	Disable WCCP setting.								
webcache *	Enable/disable web cache.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
webcache-https *	Enable/disable web cache for HTTPS.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable web cache for HTTPS.</td></tr><tr><td><i>enable</i></td><td>Enable web cache for HTTPS.</td></tr></table>	Option	Description	<i>disable</i>	Disable web cache for HTTPS.	<i>enable</i>	Enable web cache for HTTPS.		
Option	Description								
<i>disable</i>	Disable web cache for HTTPS.								
<i>enable</i>	Enable web cache for HTTPS.								
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35						
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63						
webproxy-profile	Webproxy profile name.	string	Maximum length: 63						
wssso	Enable/disable WiFi Single Sign On (WSSO).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

* This parameter may not exist in some models.

config firewall policy46

Configure IPv4 to IPv6 policies.

```
config firewall policy46
  Description: Configure IPv4 to IPv6 policies.
  edit <policyid>
    set action [accept|deny]
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set dstintf {string}
    set fixedport [enable|disable]
    set ippool [enable|disable]
    set logtraffic [enable|disable]
    set logtraffic-start [enable|disable]
    set per-ip-shaper {string}
    set permit-any-host [enable|disable]
    set poolname <name1>, <name2>, ...
    set schedule {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set status [enable|disable]
    set tcp-mss-receiver {integer}
    set tcp-mss-sender {integer}
    set traffic-shaper {string}
    set traffic-shaper-reverse {string}
    set uuid {uuid}
  next
end
```

config firewall policy46

Parameter	Description	Type	Size
action	Accept or deny traffic matching the policy.	option	-
	Option	Description	
	<i>accept</i>	Accept matching traffic.	
	<i>deny</i>	Deny matching traffic.	
comments	Comment.	var-string	Maximum length: 1023
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79
dstintf	Destination interface name.	string	Maximum length: 35
fixedport	Enable/disable fixed port for this policy.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable fixed port for this policy.	
	<i>disable</i>	Disable fixed port for this policy.	
ippool	Enable/disable use of IP Pools for source NAT.	option	-
	Option	Description	
	<i>enable</i>	Enable use of IP Pools for source NAT.	
	<i>disable</i>	Disable use of IP Pools for source NAT.	
logtraffic	Enable/disable traffic logging for this policy.	option	-
	Option	Description	
	<i>enable</i>	Enable traffic logging.	
	<i>disable</i>	Disable traffic logging.	
logtraffic-start	Record logs when a session starts and ends.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
per-ip-shaper	Per IP traffic shaper.	string	Maximum length: 35
permit-any-host	Enable/disable allowing any host.	option	-
	Option	Description	
	<i>enable</i>	Allow any host.	
	<i>disable</i>	Do not allow any host.	
policyid	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79
schedule	Schedule name.	string	Maximum length: 35

Parameter	Description	Type	Size						
service <name>	Service name. Service name.	string	Maximum length: 79						
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79						
srcintf	Source interface name.	string	Maximum length: 35						
status	Enable/disable this policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>			Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.
Option	Description								
<i>enable</i>	Enable this policy.								
<i>disable</i>	Disable this policy.								
tcp-mss-receiver	TCP Maximum Segment Size value of receiver (0 - 65535, default = 0)	integer	Minimum value: 0 Maximum value: 65535						
tcp-mss-sender	TCP Maximum Segment Size value of sender (0 - 65535, default = 0).	integer	Minimum value: 0 Maximum value: 65535						
traffic-shaper	Traffic shaper.	string	Maximum length: 35						
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified						

config firewall policy6

Configure IPv6 policies.

```
config firewall policy6
  Description: Configure IPv6 policies.
  edit <policyid>
    set action [accept|deny|...]
    set anti-replay [enable|disable]
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set application-list {string}
    set auto-asic-offload [enable|disable]
    set av-profile {string}
    set cifs-profile {string}
```

```
set comments {var-string}
set custom-log-fields <field-id1>, <field-id2>, ...
set diffserv-forward [enable|disable]
set diffserv-reverse [enable|disable]
set diffservcode-forward {user}
set diffservcode-rev {user}
set dlp-sensor {string}
set dnsfilter-profile {string}
set dsri [enable|disable]
set dstaddr <name1>, <name2>, ...
set dstaddr-negate [enable|disable]
set dstintf <name1>, <name2>, ...
set emailfilter-profile {string}
set firewall-session-dirty [check-all|check-new]
set fixedport [enable|disable]
set fsso-groups <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set http-policy-redirect [enable|disable]
set icap-profile {string}
set inbound [enable|disable]
set inspection-mode [proxy|flow]
set ippool [enable|disable]
set ips-sensor {string}
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set name {string}
set nat [enable|disable]
set natinbound [enable|disable]
set natoutbound [enable|disable]
set np-acceleration [enable|disable]
set outbound [enable|disable]
set per-ip-shaper {string}
set poolname <name1>, <name2>, ...
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set replacemsg-override-group {string}
set rsso [enable|disable]
set schedule {string}
set send-deny-packet [enable|disable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {user}
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-mirror [enable|disable]
set ssl-mirror-intf <name1>, <name2>, ...
set ssl-ssh-profile {string}
set status [enable|disable]
set tcp-mss-receiver {integer}
set tcp-mss-sender {integer}
set tcp-session-without-syn [all|data-only|...]
set timeout-send-rst [enable|disable]
```

```

set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set url-category <id1>, <id2>, ...
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set vlan-cos-fwd {integer}
set vlan-cos-rev {integer}
set vlan-filter {user}
set voip-profile {string}
set vpntunnel {string}
set waf-profile {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}

```

next

end

config firewall policy6

Parameter	Description	Type	Size
action	Policy action (allow/deny/ipsec).	option	-
	Option	Description	
	<i>accept</i>	Allows session that match the firewall policy.	
	<i>deny</i>	Blocks sessions that match the firewall policy.	
	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.	
anti-replay	Enable/disable anti-replay check.	option	-
	Option	Description	
	<i>enable</i>	Enable anti-replay check.	
	<i>disable</i>	Disable anti-replay check.	
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295
app-group <name>	Application group names. Application group names.	string	Maximum length: 79

Parameter	Description	Type	Size						
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295						
application-list	Name of an existing Application list.	string	Maximum length: 35						
auto-asic-offload *	Enable/disable policy traffic ASIC offloading.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable auto ASIC offloading.</td></tr><tr><td>disable</td><td>Disable ASIC offloading.</td></tr></table>			Option	Description	enable	Enable auto ASIC offloading.	disable	Disable ASIC offloading.
Option	Description								
enable	Enable auto ASIC offloading.								
disable	Disable ASIC offloading.								
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35						
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35						
comments	Comment.	var-string	Maximum length: 1023						
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						
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable forward (original) traffic DiffServ.</td></tr><tr><td>disable</td><td>Disable forward (original) traffic DiffServ.</td></tr></table>			Option	Description	enable	Enable forward (original) traffic DiffServ.	disable	Disable forward (original) traffic DiffServ.
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reverse (reply) traffic DiffServ.</td></tr><tr><td>disable</td><td>Disable reverse (reply) traffic DiffServ.</td></tr></table>			Option	Description	enable	Enable reverse (reply) traffic DiffServ.	disable	Disable reverse (reply) traffic DiffServ.
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						

Parameter	Description	Type	Size
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35
dsri	Enable DSRI to ignore HTTP server responses.	option	-

Option	Description

<i>enable</i>	Enable DSRI.

<i>disable</i>	Disable DSRI.

dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-

Option	Description

<i>enable</i>	Enable source address negate.

<i>disable</i>	Disable destination address negate.

dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-

Option	Description

<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.

<i>check-new</i>	Continue to allow sessions already accepted by this policy.

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

Option	Description

<i>enable</i>	Enable setting.

<i>disable</i>	Disable setting.

Parameter	Description	Type	Size						
fssso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511						
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79						
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP(S) policy redirect.</td></tr><tr><td>disable</td><td>Disable HTTP(S) policy redirect.</td></tr></table>	Option	Description	enable	Enable HTTP(S) policy redirect.	disable	Disable HTTP(S) policy redirect.		
Option	Description								
enable	Enable HTTP(S) policy redirect.								
disable	Disable HTTP(S) policy redirect.								
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35						
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>proxy</td><td>Proxy based inspection.</td></tr><tr><td>flow</td><td>Flow based inspection.</td></tr></table>	Option	Description	proxy	Proxy based inspection.	flow	Flow based inspection.		
Option	Description								
proxy	Proxy based inspection.								
flow	Flow based inspection.								
ippool	Enable to use IP Pools for source NAT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35						
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-						

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
	Option	Description									
	<i>all</i>	Log all sessions accepted or denied by this policy.									
	<i>utm</i>	Log traffic that has a security profile applied to it.									
<i>disable</i>	Disable all logging for this policy.										
logtraffic-start	Record logs when a session starts.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
name	Policy name.	string	Maximum length: 35								
nat	Enable/disable source NAT.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
np-acceleration *	Enable/disable UTM Network Processor acceleration.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable UTM Network Processor acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable UTM Network Processor acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable UTM Network Processor acceleration.	<i>disable</i>	Disable UTM Network Processor acceleration.				
	Option	Description									
	<i>enable</i>	Enable UTM Network Processor acceleration.									
<i>disable</i>	Disable UTM Network Processor acceleration.										

Parameter	Description	Type	Size						
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35						
policyid	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294						
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79						
profile-group	Name of profile group.	string	Maximum length: 35						
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.		
	Option	Description							
	<i>single</i>	Do not allow security profile groups.							
<i>group</i>	Allow security profile groups.								
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35						
rssso	Enable/disable RADIUS single sign-on (RSSO).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
schedule	Schedule name.	string	Maximum length: 35						
send-deny-packet	Enable/disable return of deny-packet.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
service <name>	Service and service group names. Address name.	string	Maximum length: 79
service-negate	When enabled service specifies what the service must NOT be.	option	-
	Option	Description	
	<i>enable</i>	Enable negated service match.	
	<i>disable</i>	Disable negated service match.	
session-ttl	Session TTL in seconds for sessions accepted by this policy. 0 means use the system default session TTL.	user	Not Specified
srcaddr <name>	Source address and address group names. Address name.	string	Maximum length: 79
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-
	Option	Description	
	<i>enable</i>	Enable source address negate.	
	<i>disable</i>	Disable destination address negate.	
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-
	Option	Description	
	<i>enable</i>	Enable SSH policy redirect.	
	<i>disable</i>	Disable SSH policy redirect.	
ssl-mirror	Enable to copy decrypted SSL traffic to a FortiGate interface (called SSL mirroring).	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable SSL mirror.	
	<i>disable</i>	Disable SSL mirror.	
ssl-mirror-intf <name>	SSL mirror interface name. Interface name.	string	Maximum length: 79
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
status	Enable or disable this policy.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-
	Option	Description	
	<i>all</i>	Enable TCP session without SYN.	
	<i>data-only</i>	Enable TCP session data only.	
	<i>disable</i>	Disable TCP session without SYN.	
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-
	Option	Description	
	<i>enable</i>	Send RST when session times out.	
	<i>disable</i>	Donot send RST when session times out.	
tos	ToS (Type of Service) value used for comparison.	user	Not Specified

Parameter	Description	Type	Size						
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TOS match negate.</td></tr><tr><td>disable</td><td>Disable TOS match negate.</td></tr></table>	Option	Description	enable	Enable TOS match negate.	disable	Disable TOS match negate.		
	Option	Description							
	enable	Enable TOS match negate.							
disable	Disable TOS match negate.								
traffic-shaper	Reverse traffic shaper.	string	Maximum length: 35						
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35						
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295						
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79						
utm-status	Enable AV/web/ips protection profile.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description							
	enable	Enable setting.							
disable	Disable setting.								
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified						
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						
vlan-filter	Set VLAN filters.	user	Not Specified						
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35						

Parameter	Description	Type	Size
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35
webcache *	Enable/disable web cache.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
webcache-https *	Enable/disable web cache for HTTPS.	option	-
	Option	Description	
	<i>disable</i>	Disable web cache for HTTPS.	
	<i>enable</i>	Enable web cache for HTTPS.	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63
webproxy-profile	Webproxy profile name.	string	Maximum length: 63

* This parameter may not exist in some models.

config firewall policy64

Configure IPv6 to IPv4 policies.

```
config firewall policy64
    Description: Configure IPv6 to IPv4 policies.
    edit <policyid>
        set action [accept|deny]
        set comments {var-string}
        set dstaddr <name1>, <name2>, ...
        set dstintf {string}
        set fixedport [enable|disable]
        set ippool [enable|disable]
        set logtraffic [enable|disable]
        set logtraffic-start [enable|disable]
        set per-ip-shaper {string}
        set permit-any-host [enable|disable]
        set poolname <name1>, <name2>, ...
        set schedule {string}
```

```

        set service <name1>, <name2>, ...
        set srcaddr <name1>, <name2>, ...
        set srcintf {string}
        set status [enable|disable]
        set tcp-mss-receiver {integer}
        set tcp-mss-sender {integer}
        set traffic-shaper {string}
        set traffic-shaper-reverse {string}
        set uuid {uuid}
    next
end

```

config firewall policy64

Parameter	Description	Type	Size
action	Policy action.	option	-
	Option	Description	
	<i>accept</i>	Action accept.	
	<i>deny</i>	Action deny.	
comments	Comment.	var-string	Maximum length: 1023
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79
dstintf	Destination interface name.	string	Maximum length: 35
fixedport	Enable/disable policy fixed port.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
ippool	Enable/disable policy64 IP pool.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
logtraffic	Enable/disable policy log traffic.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable setting.	
logtraffic-start	Record logs when a session starts and ends.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35
permit-any-host	Enable/disable permit any host in.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
policyid	Policy ID (0 - 4294967294).	integer	Minimum value: 0 Maximum value: 4294967294
poolname <name>	Policy IP pool names. IP pool name.	string	Maximum length: 79
schedule	Schedule name.	string	Maximum length: 35
service <name>	Service name. Address name.	string	Maximum length: 79
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79
srcintf	Source interface name.	string	Maximum length: 35
status	Enable/disable policy status.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size
tcp-mss-receiver	TCP MSS value of receiver.	integer	Minimum value: 0 Maximum value: 65535
tcp-mss-sender	TCP MSS value of sender.	integer	Minimum value: 0 Maximum value: 65535
traffic-shaper	Traffic shaper.	string	Maximum length: 35
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

config firewall profile-group

Configure profile groups.

```
config firewall profile-group
    Description: Configure profile groups.
    edit <name>
        set application-list {string}
        set av-profile {string}
        set cifs-profile {string}
        set dlp-sensor {string}
        set dnsfilter-profile {string}
        set emailfilter-profile {string}
        set icap-profile {string}
        set ips-sensor {string}
        set profile-protocol-options {string}
        set ssh-filter-profile {string}
        set ssl-ssh-profile {string}
        set voip-profile {string}
        set waf-profile {string}
        set webfilter-profile {string}
    next
end
```

config firewall profile-group

Parameter	Description	Type	Size
application-list	Name of an existing Application list.	string	Maximum length: 35

Parameter	Description	Type	Size
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35
dlp-sensor	Name of an existing DLP sensor.	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
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35
name	Profile group name.	string	Maximum length: 35
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35

config firewall profile-protocol-options

Configure protocol options.

```
config firewall profile-protocol-options
  Description: Configure protocol options.
  edit <name>
    config cifs
      Description: Configure CIFS protocol options.
      set ports {integer}
```

```

    set server-credential-type [none|credential-replication|...]
    config server-keytab
        Description: Server keytab.
        edit <principal>
            set keytab {string}
        next
    end
    set status [enable|disable]
end
set comment {var-string}
config dns
    Description: Configure DNS protocol options.
    set ports {integer}
    set status [enable|disable]
end
config ftp
    Description: Configure FTP protocol options.
    set comfort-amount {integer}
    set comfort-interval {integer}
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config http
    Description: Configure HTTP protocol options.
    set block-page-status-code {integer}
    set comfort-amount {integer}
    set comfort-interval {integer}
    set fortinet-bar [enable|disable]
    set fortinet-bar-port {integer}
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set post-lang {option1}, {option2}, ...
    set range-block [disable|enable]
    set retry-count {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set stream-based-uncompressed-limit {integer}
    set streaming-content-bypass [enable|disable]
    set strip-x-forwarded-for [disable|enable]
    set switching-protocols [bypass|block]
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}
    set tcp-window-size {integer}
    set tcp-window-type [system|static|...]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}

```

```

end
config imap
    Description: Configure IMAP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config mail-signature
    Description: Configure Mail signature.
    set signature {string}
    set status [disable|enable]
end
config mapi
    Description: Configure MAPI protocol options.
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config nntp
    Description: Configure NNTP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
set oversize-log [disable|enable]
config pop3
    Description: Configure POP3 protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set ports {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
set replacemsg-group {string}
set rpc-over-http [enable|disable]
config smtp
    Description: Configure SMTP protocol options.

```

```

        set inspect-all [enable|disable]
        set options {option1}, {option2}, ...
        set oversize-limit {integer}
        set ports {integer}
        set scan-bzip2 [enable|disable]
        set server-busy [enable|disable]
        set ssl-offloaded [no|yes]
        set status [enable|disable]
        set uncompressed-nest-limit {integer}
        set uncompressed-oversize-limit {integer}
    end
    config ssh
        Description: Configure SFTP and SCP protocol options.
        set comfort-amount {integer}
        set comfort-interval {integer}
        set options {option1}, {option2}, ...
        set oversize-limit {integer}
        set scan-bzip2 [enable|disable]
        set uncompressed-nest-limit {integer}
        set uncompressed-oversize-limit {integer}
    end
    set switching-protocols-log [disable|enable]
next
end

```

config firewall profile-protocol-options

Parameter	Description	Type	Size
comment	Optional comments.	var-string	Maximum length: 255
name	Name.	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.	
replacemsg-group	Name of the replacement message group to be used	string	Maximum length: 35
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-
	Option	Description	
	enable	Enable inspection of RPC over HTTP.	
	disable	Disable inspection of RPC over HTTP.	

Parameter	Description	Type	Size
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-

Option	Description
<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.
<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.

config cifs

Parameter	Description	Type	Size
ports	Ports to scan for content (1 - 65535, default = 445).	integer	Minimum value: 1 Maximum value: 65535
server-credential-type	CIFS server credential type.	option	-

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

status	Enable/disable the active status of scanning for this protocol.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config server-keytab

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

config dns

Parameter	Description	Type	Size
ports	Ports to scan for content (1 - 65535, default = 53).	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable the active status of scanning for this protocol.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config ftp

Parameter	Description	Type	Size
comfort-amount	Amount of data to send in a transmission for client comforting (1 - 65535 bytes, default = 1).	integer	Minimum value: 1 Maximum value: 65535
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data (1 - 900 sec, default = 10).	integer	Minimum value: 1 Maximum value: 900
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

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

Option	Description
<i>clientcomfort</i>	Prevent client timeout.
<i>oversize</i>	Block oversized file/email.
<i>splice</i>	Enable splice mode.
<i>bypass-rest-command</i>	Bypass REST command.

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass-mode-command</i></td><td>Bypass MODE command.</td></tr></table>	Option	Description	<i>bypass-mode-command</i>	Bypass MODE command.				
	Option	Description							
<i>bypass-mode-command</i>	Bypass MODE command.								
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **						
ports	Ports to scan for content (1 - 65535, default = 21).	integer	Minimum value: 1 Maximum value: 65535						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.		
	Option	Description							
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.							
<i>yes</i>	SSL decryption and encryption performed by an external device.								
status	Enable/disable the active status of scanning for this protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **						

** Values may differ between models.

config http

Parameter	Description	Type	Size										
block-page-status-code	Code number returned for blocked HTTP pages (non-FortiGuard only) (100 - 599, default = 403).	integer	Minimum value: 100 Maximum value: 599										
comfort-amount	Amount of data to send in a transmission for client comforting (1 - 65535 bytes, default = 1).	integer	Minimum value: 1 Maximum value: 65535										
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data (1 - 900 sec, default = 10).	integer	Minimum value: 1 Maximum value: 900										
fortinet-bar	Enable/disable Fortinet bar on HTML content.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
Option	Description												
<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.												
fortinet-bar-port	Port for use by Fortinet Bar (1 - 65535, default = 8011).	integer	Minimum value: 1 Maximum value: 65535										
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
Option	Description												
<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.												
options	One or more options that can be applied to the session.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clientcomfort</i></td><td>Prevent client timeout.</td></tr><tr><td><i>servercomfort</i></td><td>Prevent server timeout.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file/email.</td></tr><tr><td><i>chunkedbypass</i></td><td>Bypass chunked transfer encoded sites.</td></tr></table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.	<i>oversize</i>	Block oversized file/email.	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.		
Option	Description												
<i>clientcomfort</i>	Prevent client timeout.												
<i>servercomfort</i>	Prevent server timeout.												
<i>oversize</i>	Block oversized file/email.												
<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.												

Parameter	Description	Type	Size
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **
ports	Ports to scan for content (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-

Option	Description
<i>jisx0201</i>	Japanese Industrial Standard 0201.
<i>jisx0208</i>	Japanese Industrial Standard 0208.
<i>jisx0212</i>	Japanese Industrial Standard 0212.
<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).
<i>ksc5601-ex</i>	Wansung Korean standard 5601.
<i>euc-jp</i>	Extended Unicode Japanese.
<i>sjis</i>	Shift Japanese Industrial Standard.
<i>iso2022-jp</i>	ISO 2022 Japanese.
<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.
<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.
<i>euc-cn</i>	Extended Unicode Chinese.
<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).
<i>hz</i>	Hanzi simplified Chinese.
<i>ces-big5</i>	Big-5 traditional Chinese.
<i>euc-kr</i>	Extended Unicode Korean.
<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.
<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).
<i>tis620</i>	Thai Industrial Standard 620.
<i>cp874</i>	Code Page 874 (Thai).
<i>cp1252</i>	Code Page 1252 (Western European Latin).
<i>cp1251</i>	Code Page 1251 (Cyrillic).

Parameter	Description	Type	Size						
range-block	Enable/disable blocking of partial downloads.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable blocking of partial downloads.</td></tr><tr><td><i>enable</i></td><td>Enable blocking of partial downloads.</td></tr></table>	Option	Description	<i>disable</i>	Disable blocking of partial downloads.	<i>enable</i>	Enable blocking of partial downloads.		
Option	Description								
<i>disable</i>	Disable blocking of partial downloads.								
<i>enable</i>	Enable blocking of partial downloads.								
retry-count	Number of attempts to retry HTTP connection (0 - 100, default = 0).	integer	Minimum value: 0 Maximum value: 100						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.		
Option	Description								
<i>no</i>	SSL decryption and encryption performed by FortiGate when deep inspection is enabled.								
<i>yes</i>	SSL decryption and encryption performed by an external device.								
status	Enable/disable the active status of scanning for this protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned (MB, 0 = unlimited (default). Stream-based uncompression used only under certain conditions.).	integer	Minimum value: 0 Maximum value: 4294967295						
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-						

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

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

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

switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-

Option	Description
<i>bypass</i>	Bypass connections when switching protocols.
<i>block</i>	Block connections when switching protocols.

tcp-window-maximum	Maximum dynamic TCP window size (default = 8MB).	integer	Minimum value: 1048576 Maximum value: 33554432

tcp-window-minimum	Minimum dynamic TCP window size (default = 128KB).	integer	Minimum value: 65536 Maximum value: 1048576

tcp-window-size	Set TCP static window size (default = 256KB).	integer	Minimum value: 65536 Maximum value: 33554432

tcp-window-type	Specify type of TCP window to use for this protocol.	option	-

Option	Description
<i>system</i>	Use system default TCP window size for this protocol (Default).
<i>static</i>	Manually specify TCP window size.
<i>dynamic</i>	Vary TCP window size based on available memory, within limits.

Parameter	Description	Type	Size
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **

** Values may differ between models.

config imap

Parameter	Description	Type	Size						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
options	One or more options that can be applied to the session.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file/email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.		
Option	Description								
<i>fragmail</i>	Pass fragmented email.								
<i>oversize</i>	Block oversized file/email.								
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **						
ports	Ports to scan for content (1 - 65535, default = 143).	integer	Minimum value: 1 Maximum value: 65535						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size						
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiGate when deep inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	no	SSL decryption and encryption performed by FortiGate when deep inspection is enabled.	yes	SSL decryption and encryption performed by an external device.		
Option	Description								
no	SSL decryption and encryption performed by FortiGate when deep inspection is enabled.								
yes	SSL decryption and encryption performed by an external device.								
status	Enable/disable the active status of scanning for this protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **						

** Values may differ between models.

config mail-signature

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

config mapi

Parameter	Description	Type	Size						
options	One or more options that can be applied to the session.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file/email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.		
Option	Description								
<i>fragmail</i>	Pass fragmented email.								
<i>oversize</i>	Block oversized file/email.								
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **						
ports	Ports to scan for content (1 - 65535, default = 135).	integer	Minimum value: 1 Maximum value: 65535						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
status	Enable/disable the active status of scanning for this protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **						

** Values may differ between models.

config nntp

Parameter	Description	Type	Size						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
options	One or more options that can be applied to the session.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>oversize</i></td><td>Block oversized file/email.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr></table>	Option	Description	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.		
Option	Description								
<i>oversize</i>	Block oversized file/email.								
<i>splice</i>	Enable splice mode.								
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **						
ports	Ports to scan for content (1 - 65535, default = 119).	integer	Minimum value: 1 Maximum value: 65535						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
status	Enable/disable the active status of scanning for this protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100						

Parameter	Description	Type	Size
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **

** Values may differ between models.

config pop3

Parameter	Description	Type	Size						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
options	One or more options that can be applied to the session.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file/email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.		
Option	Description								
<i>fragmail</i>	Pass fragmented email.								
<i>oversize</i>	Block oversized file/email.								
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **						
ports	Ports to scan for content (1 - 65535, default = 110).	integer	Minimum value: 1 Maximum value: 65535						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.		
	Option	Description							
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.							
<i>yes</i>	SSL decryption and encryption performed by an external device.								
status	Enable/disable the active status of scanning for this protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **						

** Values may differ between models.

config smtp

Parameter	Description	Type	Size								
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
options	One or more options that can be applied to the session.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file/email.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized file/email.	<i>splice</i>	Enable splice mode.		
Option	Description										
<i>fragmail</i>	Pass fragmented email.										
<i>oversize</i>	Block oversized file/email.										
<i>splice</i>	Enable splice mode.										

Parameter	Description	Type	Size
oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **
ports	Ports to scan for content (1 - 65535, default = 25).	integer	Minimum value: 1 Maximum value: 65535
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.	
status	Enable/disable the active status of scanning for this protocol.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100

Parameter	Description	Type	Size
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **

** Values may differ between models.

config ssh

Parameter	Description	Type	Size
comfort-amount	Amount of data to send in a transmission for client comforting (1 - 65535 bytes, default = 1).	integer	Minimum value: 1 Maximum value: 65535
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data (1 - 900 sec, default = 10).	integer	Minimum value: 1 Maximum value: 900
options	One or more options that can be applied to the session.	option	-

Option	Description
<i>oversize</i>	Block oversized file/email.
<i>clientcomfort</i>	Prevent client timeout.
<i>servercomfort</i>	Prevent server timeout.

oversize-limit	Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10).	integer	Minimum value: 1 Maximum value: 1606 **
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default = 12).	integer	Minimum value: 2 Maximum value: 100

Parameter	Description	Type	Size
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited, default = 10).	integer	Minimum value: 0 Maximum value: 1606 **

** Values may differ between models.

config firewall proxy-address

Configure web proxy address.

```
config firewall proxy-address
  Description: Configure web proxy address.
  edit <name>
    set case-sensitivity [disable|enable]
    set category <id1>, <id2>, ...
    set color {integer}
    set comment {var-string}
    set header {string}
    config header-group
      Description: HTTP header group.
      edit <id>
        set case-sensitivity [disable|enable]
        set header {string}
        set header-name {string}
      next
    end
    set header-name {string}
    set host {string}
    set host-regex {string}
    set method {option1}, {option2}, ...
    set path {string}
    set query {string}
    set referrer [enable|disable]
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set type [host-regex|url|...]
    set ua {option1}, {option2}, ...
    set uuid {uuid}
    set visibility [enable|disable]
  next
end
```

config firewall proxy-address

Parameter	Description	Type	Size														
case-sensitivity	Enable to make the pattern case sensitive.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Case insensitive in pattern.</td></tr><tr><td><i>enable</i></td><td>Case sensitive in pattern.</td></tr></table>			Option	Description	<i>disable</i>	Case insensitive in pattern.	<i>enable</i>	Case sensitive in pattern.								
Option	Description																
<i>disable</i>	Case insensitive in pattern.																
<i>enable</i>	Case sensitive in pattern.																
category <id>	FortiGuard category ID. Fortiguard category id.	integer	Minimum value: 0 Maximum value: 4294967295														
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1).	integer	Minimum value: 0 Maximum value: 32														
comment	Optional comments.	var-string	Maximum length: 255														
header	HTTP header name as a regular expression.	string	Maximum length: 255														
header-name	Name of HTTP header.	string	Maximum length: 79														
host	Address object for the host.	string	Maximum length: 79														
host-regex	Host name as a regular expression.	string	Maximum length: 255														
method	HTTP request methods to be used.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>get</i></td><td>GET method.</td></tr><tr><td><i>post</i></td><td>POST method.</td></tr><tr><td><i>put</i></td><td>PUT method.</td></tr><tr><td><i>head</i></td><td>HEAD method.</td></tr><tr><td><i>connect</i></td><td>CONNECT method.</td></tr><tr><td><i>trace</i></td><td>TRACE method.</td></tr></table>			Option	Description	<i>get</i>	GET method.	<i>post</i>	POST method.	<i>put</i>	PUT method.	<i>head</i>	HEAD method.	<i>connect</i>	CONNECT method.	<i>trace</i>	TRACE method.
Option	Description																
<i>get</i>	GET method.																
<i>post</i>	POST method.																
<i>put</i>	PUT method.																
<i>head</i>	HEAD method.																
<i>connect</i>	CONNECT method.																
<i>trace</i>	TRACE method.																

Parameter	Description	Type	Size
	Option	Description	
	<i>options</i>	OPTIONS method.	
	<i>delete</i>	DELETE method.	
name	Address name.	string	Maximum length: 35
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	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
type	Proxy address type.	option	-
	Option	Description	
	<i>host-regex</i>	Host regular expression.	
	<i>url</i>	HTTP URL.	
	<i>category</i>	FortiGuard URL category.	
	<i>method</i>	HTTP request method.	
	<i>ua</i>	HTTP request user agent.	
	<i>header</i>	HTTP request header.	
	<i>src-advanced</i>	HTTP advanced source criteria.	
	<i>dst-advanced</i>	HTTP advanced destination criteria.	
ua	Names of browsers to be used as user agent.	option	-
	Option	Description	
	<i>chrome</i>	Google Chrome.	
	<i>ms</i>	Microsoft Internet Explorer or EDGE.	
	<i>firefox</i>	Mozilla Firefox.	
	<i>safari</i>	Apple Safari.	

Parameter	Description	Type	Size
	Option	Description	
	<i>other</i>	Other browsers.	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable visibility of the object in the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config header-group

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

config tagging

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

config firewall proxy-addrgrp

Configure web proxy address group.

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

config firewall proxy-addrgrp

Parameter	Description	Type	Size
color	Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1).	integer	Minimum value: 0 Maximum value: 32
comment	Optional comments.	var-string	Maximum length: 255
member <name>	Members of address group. Address name.	string	Maximum length: 79
name	Address group name.	string	Maximum length: 63
type	Source or destination address group type.	option	-
		Option	Description
		<i>src</i>	Source group.
		<i>dst</i>	Destination group.
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable visibility of the object in the GUI.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config tagging

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

config firewall proxy-policy

Configure proxy policies.

```
config firewall proxy-policy
    Description: Configure proxy policies.
    edit <policyid>
        set action [accept|deny|...]
        set application-list {string}
        set av-profile {string}
        set cifs-profile {string}
        set comments {var-string}
        set disclaimer [disable|domain|...]
        set dlp-sensor {string}
        set dstaddr <name1>, <name2>, ...
        set dstaddr-negate [enable|disable]
        set dstaddr6 <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set emailfilter-profile {string}
        set groups <name1>, <name2>, ...
        set http-tunnel-auth [enable|disable]
        set icap-profile {string}
        set internet-service [enable|disable]
        set internet-service-custom <name1>, <name2>, ...
        set internet-service-custom-group <name1>, <name2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-id <id1>, <id2>, ...
        set internet-service-negate [enable|disable]
        set ips-sensor {string}
        set logtraffic [all|utm|...]
        set logtraffic-start [enable|disable]
```

```

set poolname <name1>, <name2>, ...
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set proxy [explicit-web|transparent-web|...]
set redirect-url {var-string}
set replacemsg-override-group {string}
set schedule {string}
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {integer}
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-ssh-profile {string}
set status [enable|disable]
set transparent [enable|disable]
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set waf-profile {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}

```

next

end

config firewall proxy-policy

Parameter	Description	Type	Size								
action	Accept or deny traffic matching the policy parameters.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Action accept.</td></tr><tr><td><i>deny</i></td><td>Action deny.</td></tr><tr><td><i>redirect</i></td><td>Action redirect.</td></tr></table>			Option	Description	<i>accept</i>	Action accept.	<i>deny</i>	Action deny.	<i>redirect</i>	Action redirect.
	Option	Description									
	<i>accept</i>	Action accept.									
	<i>deny</i>	Action deny.									
	<i>redirect</i>	Action redirect.									
application-list	Name of an existing Application list.	string	Maximum length: 35								
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35								

Parameter	Description	Type	Size										
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35										
comments	Optional comments.	var-string	Maximum length: 1023										
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable disclaimer.</td></tr><tr><td><i>domain</i></td><td>Display disclaimer for domain</td></tr><tr><td><i>policy</i></td><td>Display disclaimer for policy</td></tr><tr><td><i>user</i></td><td>Display disclaimer for current user</td></tr></table>	Option	Description	<i>disable</i>	Disable disclaimer.	<i>domain</i>	Display disclaimer for domain	<i>policy</i>	Display disclaimer for policy	<i>user</i>	Display disclaimer for current user		
Option	Description												
<i>disable</i>	Disable disclaimer.												
<i>domain</i>	Display disclaimer for domain												
<i>policy</i>	Display disclaimer for policy												
<i>user</i>	Display disclaimer for current user												
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35										
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79										
dstaddr-negate	When enabled, destination addresses match against any address EXCEPT the specified destination addresses.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable destination address negate.						
Option	Description												
<i>enable</i>	Enable source address negate.												
<i>disable</i>	Disable destination address negate.												
dstaddr6 <name>	IPv6 destination address objects. Address name.	string	Maximum length: 79										
dstintf <name>	Destination interface names. Interface name.	string	Maximum length: 79										
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35										
groups <name>	Names of group objects. Group name.	string	Maximum length: 79										
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-										

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-
	Option	Description	
	<i>enable</i>	Enable use of Internet Services in policy.	
	<i>disable</i>	Disable use of Internet Services in policy.	
internet-service-custom <name>	Custom Internet Service name. Custom name.	string	Maximum length: 79
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79
internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295
internet-service-negate	When enabled, Internet Services match against any internet service EXCEPT the selected Internet Service.	option	-
	Option	Description	
	<i>enable</i>	Enable negated Internet Service match.	
	<i>disable</i>	Disable negated Internet Service match.	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35
logtraffic	Enable/disable logging traffic through the policy.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions.</td></tr><tr><td><i>utm</i></td><td>UTM event and matched application traffic log.</td></tr><tr><td><i>disable</i></td><td>Disable traffic and application log.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions.	<i>utm</i>	UTM event and matched application traffic log.	<i>disable</i>	Disable traffic and application log.				
	Option	Description											
	<i>all</i>	Log all sessions.											
	<i>utm</i>	UTM event and matched application traffic log.											
<i>disable</i>	Disable traffic and application log.												
logtraffic-start	Enable/disable policy log traffic start.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295										
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79										
profile-group	Name of profile group.	string	Maximum length: 35										
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35										
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.						
	Option	Description											
	<i>single</i>	Do not allow security profile groups.											
<i>group</i>	Allow security profile groups.												
proxy	Type of explicit proxy.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>explicit-web</i></td><td>Explicit Web Proxy</td></tr><tr><td><i>transparent-web</i></td><td>Transparent Web Proxy</td></tr><tr><td><i>ftp</i></td><td>Explicit FTP Proxy</td></tr><tr><td><i>ssh</i></td><td>SSH Proxy</td></tr></table>	Option	Description	<i>explicit-web</i>	Explicit Web Proxy	<i>transparent-web</i>	Transparent Web Proxy	<i>ftp</i>	Explicit FTP Proxy	<i>ssh</i>	SSH Proxy		
	Option	Description											
	<i>explicit-web</i>	Explicit Web Proxy											
	<i>transparent-web</i>	Transparent Web Proxy											
	<i>ftp</i>	Explicit FTP Proxy											
<i>ssh</i>	SSH Proxy												

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssh-tunnel</i></td><td>SSH Tunnel</td></tr><tr><td><i>wanopt</i></td><td>WANopt Tunnel</td></tr></table>	Option	Description	<i>ssh-tunnel</i>	SSH Tunnel	<i>wanopt</i>	WANopt Tunnel		
	Option	Description							
	<i>ssh-tunnel</i>	SSH Tunnel							
<i>wanopt</i>	WANopt Tunnel								
redirect-url	Redirect URL for further explicit web proxy processing.	var-string	Maximum length: 1023						
replacemsg-override-group	Authentication replacement message override group.	string	Maximum length: 35						
schedule	Name of schedule object.	string	Maximum length: 35						
service <name>	Name of service objects. Service name.	string	Maximum length: 79						
service-negate	When enabled, services match against any service EXCEPT the specified destination services.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.		
	Option	Description							
	<i>enable</i>	Enable negated service match.							
<i>disable</i>	Disable negated service match.								
session-ttl	TTL in seconds for sessions accepted by this policy (0 means use the system default session TTL).	integer	Minimum value: 300 Maximum value: 2764800						
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79						
srcaddr-negate	When enabled, source addresses match against any address EXCEPT the specified source addresses.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable destination address negate.		
	Option	Description							
	<i>enable</i>	Enable source address negate.							
<i>disable</i>	Disable destination address negate.								
srcaddr6 <name>	IPv6 source address objects. Address name.	string	Maximum length: 79						
srcintf <name>	Source interface names. Interface name.	string	Maximum length: 79						
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35						

Parameter	Description	Type	Size						
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable SSH policy redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH policy redirect.	<i>disable</i>	Disable SSH policy redirect.		
Option	Description								
<i>enable</i>	Enable SSH policy redirect.								
<i>disable</i>	Disable SSH policy redirect.								
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35						
status	Enable/disable the active status of the policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
transparent	Enable to use the IP address of the client to connect to the server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of IP address of client to connect to server.</td></tr><tr><td><i>disable</i></td><td>Disable use of IP address of client to connect to server.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of IP address of client to connect to server.	<i>disable</i>	Disable use of IP address of client to connect to server.		
Option	Description								
<i>enable</i>	Enable use of IP address of client to connect to server.								
<i>disable</i>	Disable use of IP address of client to connect to server.								
users <name>	Names of user objects. Group name.	string	Maximum length: 79						
utm-status	Enable the use of UTM profiles/sensors/lists.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified						
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35						
webcache *	Enable/disable web caching.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size
webcache-https *	Enable/disable web caching for HTTPS (Requires deep-inspection enabled in ssl-ssh-profile).	option	-
	Option	Description	
	disable	Disable web cache for HTTPS.	
	enable	Enable web cache for HTTPS.	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35
webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63
webproxy-profile	Name of web proxy profile.	string	Maximum length: 63

* This parameter may not exist in some models.

config firewall schedule group

Schedule group configuration.

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

config firewall schedule group

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

config firewall schedule onetime

Onetime schedule configuration.

```
config firewall schedule onetime
  Description: Onetime schedule configuration.
  edit <name>
    set color {integer}
    set end {user}
    set expiration-days {integer}
    set start {user}
  next
end
```

config firewall schedule onetime

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100
name	Onetime schedule name.	string	Maximum length: 31
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified

config firewall schedule recurring

Recurring schedule configuration.

```
config firewall schedule recurring
  Description: Recurring schedule configuration.
  edit <name>
    set color {integer}
    set day {option1}, {option2}, ...
    set end {user}
    set start {user}
  next
end
```

config firewall schedule recurring

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
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	
	<i>sunday</i>	Sunday.	
	<i>monday</i>	Monday.	
	<i>tuesday</i>	Tuesday.	
	<i>wednesday</i>	Wednesday.	
	<i>thursday</i>	Thursday.	
	<i>friday</i>	Friday.	
	<i>saturday</i>	Saturday.	
	<i>none</i>	None.	
end	Time of day to end the schedule, format hh:mm.	user	Not Specified
name	Recurring schedule name.	string	Maximum length: 31
start	Time of day to start the schedule, format hh:mm.	user	Not Specified

config firewall security-policy

Configure NGFW IPv4/IPv6 application policies.

```
config firewall security-policy
  Description: Configure NGFW IPv4/IPv6 application policies.
  edit <policyid>
    set action [accept|deny]
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set application-list {string}
    set av-profile {string}
    set cifs-profile {string}
    set comments {var-string}
    set dlp-sensor {string}
```

```

set dnsfilter-profile {string}
set dstaddr4 <name1>, <name2>, ...
set dstaddr6 <name1>, <name2>, ...
set dstintf <name1>, <name2>, ...
set emailfilter-profile {string}
set enforce-default-app-port [enable|disable]
set fsso-groups <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set icap-profile {string}
set internet-service [enable|disable]
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-id <id1>, <id2>, ...
set internet-service-negate [enable|disable]
set internet-service-src [enable|disable]
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-id <id1>, <id2>, ...
set internet-service-src-negate [enable|disable]
set ips-sensor {string}
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set name {string}
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set schedule {string}
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set srcaddr4 <name1>, <name2>, ...
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssl-ssh-profile {string}
set status [enable|disable]
set url-category <id1>, <id2>, ...
set users <name1>, <name2>, ...
set uuid {uuid}
set voip-profile {string}
set webfilter-profile {string}

```

next

end

config firewall security-policy

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

Parameter	Description	Type	Size

	Option	Description	
	<i>accept</i>	Allows session that match the firewall policy.	
	<i>deny</i>	Blocks sessions that match the firewall policy.	

app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295
app-group <name>	Application group names. Application group names.	string	Maximum length: 79
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295
application-list	Name of an existing Application list.	string	Maximum length: 35
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35
comments	Comment.	var-string	Maximum length: 1023
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35
dstaddr4 <name>	Destination IPv4 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
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79
emailfilter- profile	Name of an existing email filter profile.	string	Maximum length: 35

Parameter	Description	Type	Size						
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511						
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79						
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35						
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.		
Option	Description								
<i>enable</i>	Enable use of Internet Services in policy.								
<i>disable</i>	Disable use of Internet Services in policy.								
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79						
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79						
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79						
internet-service-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	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable negated Internet Service match.	
	<i>disable</i>	Disable negated Internet Service match.	
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-
	Option	Description	
	<i>enable</i>	Enable use of Internet Services source in policy.	
	<i>disable</i>	Disable use of Internet Services source in policy.	
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79
internet-service-src-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	
	<i>enable</i>	Enable negated Internet Service source match.	
	<i>disable</i>	Disable negated Internet Service source match.	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.		
	Option	Description									
	<i>all</i>	Log all sessions accepted or denied by this policy.									
	<i>utm</i>	Log traffic that has a security profile applied to it.									
<i>disable</i>	Disable all logging for this policy.										
logtraffic-start	Record logs when a session starts.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description									
	<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.										
name	Policy name.	string	Maximum length: 35								
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294								
profile-group	Name of profile group.	string	Maximum length: 35								
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35								
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.				
	Option	Description									
	<i>single</i>	Do not allow security profile groups.									
<i>group</i>	Allow security profile groups.										
schedule	Schedule name.	string	Maximum length: 35								
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable deny-packet sending.</td></tr><tr><td><i>enable</i></td><td>Enable deny-packet sending.</td></tr></table>	Option	Description	<i>disable</i>	Disable deny-packet sending.	<i>enable</i>	Enable deny-packet sending.				
	Option	Description									
	<i>disable</i>	Disable deny-packet sending.									
<i>enable</i>	Enable deny-packet sending.										

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated service match.</td></tr><tr><td>disable</td><td>Disable negated service match.</td></tr></table>	Option	Description	enable	Enable negated service match.	disable	Disable negated service match.		
Option	Description								
enable	Enable negated service match.								
disable	Disable negated service match.								
srcaddr4 <name>	Source 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						
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79						
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35						
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35						
status	Enable or disable this policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295						
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified						
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35						

Parameter	Description	Type	Size
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35

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
name	Service category name.	string	Maximum length: 63

config firewall service custom

Configure custom services.

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

```

        set tcp-halfclose-timer {integer}
        set tcp-halfopen-timer {integer}
        set tcp-portrange {user}
        set tcp-timewait-timer {integer}
        set udp-idle-timer {integer}
        set udp-portrange {user}
        set visibility [enable|disable]
    next
end

```

config firewall service custom

Parameter	Description	Type	Size
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295
app-service- type	Application service type.	option	-
	Option	Description	
	<i>disable</i>	Disable application type.	
	<i>app-id</i>	Application ID.	
	<i>app-category</i>	Applicatin category.	
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295
category	Service category.	string	Maximum length: 63
check-reset- range	Configure the type of ICMP error message verification.	option	-
	Option	Description	
	<i>disable</i>	Disable RST range check.	
	<i>strict</i>	Check RST range strictly.	
	<i>default</i>	Using system default setting.	

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
fqdn	Fully qualified domain name.	string	Maximum length: 255
helper	Helper name.	option	-

Option	Description
<i>auto</i>	Automatically select helper based on protocol and port.
<i>disable</i>	Disable helper.
<i>ftp</i>	FTP.
<i>tftp</i>	TFTP.
<i>ras</i>	RAS.
<i>h323</i>	H323.
<i>tns</i>	TNS.
<i>mms</i>	MMS.
<i>sip</i>	SIP.
<i>pptp</i>	PPTP.
<i>rtsp</i>	RTSP.
<i>dns-udp</i>	DNS UDP.
<i>dns-tcp</i>	DNS TCP.
<i>pmap</i>	PMAP.
<i>rsh</i>	RSH.
<i>dcerpc</i>	DCERPC.
<i>mgcp</i>	MGCP.

icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255

Parameter	Description	Type	Size
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295
iprange	Start and end of the IP range associated with service.	user	Not Specified
name	Custom service name.	string	Maximum length: 79
protocol	Protocol type based on IANA numbers.	option	-

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

protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254
proxy	Enable/disable web proxy service.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

sctp-portrange	Multiple SCTP port ranges.	user	Not Specified
session-ttl	Session TTL (300 - 2764800, 0 = default).	user	Not Specified

Parameter	Description	Type	Size
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet (1 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet (1 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400
tcp-portrange	Multiple TCP port ranges.	user	Not Specified
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds (1 - 300 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 300
udp-idle-timer	UDP half close timeout (0 - 86400 sec, 0 = default).	integer	Minimum value: 0 Maximum value: 86400
udp-portrange	Multiple UDP port ranges.	user	Not Specified
visibility	Enable/disable the visibility of the service on the GUI.	option	-

Option	Description
<i>enable</i>	Show in service selection.
<i>disable</i>	Hide from service selection.

config firewall service group

Configure service groups.

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

config firewall service group

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

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config firewall shaper per-ip-shaper

Configure per-IP traffic shaper.

```
config firewall shaper per-ip-shaper
  Description: Configure per-IP traffic shaper.
  edit <name>
    set bandwidth-unit [kbps|mbps|...]
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set max-bandwidth {integer}
    set max-concurrent-session {integer}
  next
end
```

config firewall shaper per-ip-shaper

Parameter	Description	Type	Size
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kbps</i></td><td>Kilobits per second.</td></tr><tr><td><i>mbps</i></td><td>Megabits per second.</td></tr><tr><td><i>gbps</i></td><td>Gigabits per second.</td></tr></table>	Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.		
	Option	Description									
	<i>kbps</i>	Kilobits per second.									
	<i>mbps</i>	Megabits per second.									
<i>gbps</i>	Gigabits per second.										
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting forward (original) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting forward (original) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting forward (original) traffic DiffServ.	<i>disable</i>	Disable setting forward (original) traffic DiffServ.				
	Option	Description									
	<i>enable</i>	Enable setting forward (original) traffic DiffServ.									
<i>disable</i>	Disable setting forward (original) traffic DiffServ.										
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting reverse (reply) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting reverse (reply) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.				
	Option	Description									
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.									
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.										
diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified								
diffservcode-rev	Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified								
max-bandwidth	Upper bandwidth limit enforced by this shaper (0 - 16776000). 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000								
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper (0 - 2097000). 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000								
name	Traffic shaper name.	string	Maximum length: 35								

config firewall shaper traffic-shaper

Configure shared traffic shaper.


```

config firewall shaper traffic-shaper
  Description: Configure shared traffic shaper.
  edit <name>
    set bandwidth-unit [kbps|mbps|...]
    set diffserv [enable|disable]
    set diffservcode {user}
    set dscp-marking-method [multi-stage|static]
    set exceed-bandwidth {integer}
    set exceed-class-id {integer}
    set exceed-dscp {user}
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
    set maximum-dscp {user}
    set overhead {integer}
    set per-policy [disable|enable]
    set priority [low|medium|...]
  next
end

```

config firewall shaper traffic-shaper

Parameter	Description	Type	Size								
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kbps</i></td><td>Kilobits per second.</td></tr><tr><td><i>mbps</i></td><td>Megabits per second.</td></tr><tr><td><i>gbps</i></td><td>Gigabits per second.</td></tr></table>	Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.		
Option	Description										
<i>kbps</i>	Kilobits per second.										
<i>mbps</i>	Megabits per second.										
<i>gbps</i>	Gigabits per second.										
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting traffic DiffServ.	<i>disable</i>	Disable setting traffic DiffServ.				
Option	Description										
<i>enable</i>	Enable setting traffic DiffServ.										
<i>disable</i>	Disable setting traffic DiffServ.										
diffservcode	DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified								
dscp-marking-method	Select DSCP marking method.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multi-stage</i></td><td>Multistage marking.</td></tr><tr><td><i>static</i></td><td>Static marking.</td></tr></table>	Option	Description	<i>multi-stage</i>	Multistage marking.	<i>static</i>	Static marking.				
Option	Description										
<i>multi-stage</i>	Multistage marking.										
<i>static</i>	Static marking.										

Parameter	Description	Type	Size						
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-class-id	Class ID for traffic in [guaranteed-bandwidth, maximum-bandwidth].	integer	Minimum value: 0 Maximum value: 4294967295						
exceed-dscp	DSCP mark for traffic in [guaranteed-bandwidth, exceed-bandwidth].	user	Not Specified						
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper (0 - 16776000). Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000						
maximum-bandwidth	Upper bandwidth limit enforced by this shaper (0 - 16776000). 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 16776000						
maximum-dscp	DSCP mark for traffic in [exceed-bandwidth, maximum-bandwidth].	user	Not Specified						
name	Traffic shaper name.	string	Maximum length: 35						
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 Maximum value: 100						
per-policy	Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>All referring policies share one traffic shaper.</td></tr><tr><td><i>enable</i></td><td>Each referring policy has its own traffic shaper.</td></tr></table>			Option	Description	<i>disable</i>	All referring policies share one traffic shaper.	<i>enable</i>	Each referring policy has its own traffic shaper.
	Option	Description							
	<i>disable</i>	All referring policies share one traffic shaper.							
<i>enable</i>	Each referring policy has its own traffic shaper.								
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-						

Parameter	Description	Type	Size

Option	Description
<i>low</i>	Low priority.
<i>medium</i>	Medium priority.
<i>high</i>	High priority.

config firewall shaping-policy

Configure shaping policies.

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

```

    set url-category <id1>, <id2>, ...
    set users <name1>, <name2>, ...
next
end

```

config firewall shaping-policy

Parameter	Description	Type	Size						
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295						
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79						
application <id>	IDs of one or more applications that this shaper applies application control traffic shaping to. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295						
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295						
comment	Comments.	var-string	Maximum length: 255						
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting forward (original) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting forward (original) traffic DiffServ.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting forward (original) traffic DiffServ.	<i>disable</i>	Disable setting forward (original) traffic DiffServ.
Option	Description								
<i>enable</i>	Enable setting forward (original) traffic DiffServ.								
<i>disable</i>	Disable setting forward (original) traffic DiffServ.								
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting reverse (reply) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting reverse (reply) traffic DiffServ.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.
Option	Description								
<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.								
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.								
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified						

Parameter	Description	Type	Size
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified
dstaddr <name>	IPv4 destination address and address group names. Address name.	string	Maximum length: 79
dstaddr6 <name>	IPv6 destination address and address group names. Address name.	string	Maximum length: 79
dstintf <name>	One or more outgoing (egress) interfaces. Interface name.	string	Maximum length: 79
groups <name>	Apply this traffic shaping policy to user groups that have authenticated with the FortiGate. Group name.	string	Maximum length: 79
id	Shaping policy ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-

Option	Description
<i>enable</i>	Enable use of Internet Service in shaping-policy.
<i>disable</i>	Disable use of Internet Service in shaping-policy.

internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79
internet-service-id <id>	Internet Service ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size						
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of Internet Service source in shaping-policy.</td></tr><tr><td>disable</td><td>Disable use of Internet Service source in shaping-policy.</td></tr></table>	Option	Description	enable	Enable use of Internet Service source in shaping-policy.	disable	Disable use of Internet Service source in shaping-policy.		
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-custom<name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79						
internet-service-src-custom-group<name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79						
internet-service-src-group<name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79						
internet-service-src-id<id>	Internet Service source ID. Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295						
ip-version	Apply this traffic shaping policy to IPv4 or IPv6 traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for Configuration Method.</td></tr><tr><td>6</td><td>Use IPv6 addressing for Configuration Method.</td></tr></table>	Option	Description	4	Use IPv4 addressing for Configuration Method.	6	Use IPv6 addressing for Configuration Method.		
Option	Description								
4	Use IPv4 addressing for Configuration Method.								
6	Use IPv6 addressing for Configuration Method.								
name	Shaping policy name.	string	Maximum length: 35						
per-ip-shaper	Per-IP traffic shaper to apply with this policy.	string	Maximum length: 35						
schedule	Schedule name.	string	Maximum length: 35						
service<name>	Service and service group names. Service name.	string	Maximum length: 79						
srcaddr<name>	IPv4 source address and address group names. Address name.	string	Maximum length: 79						

Parameter	Description	Type	Size						
srcaddr6 <name>	IPv6 source address and address group names. Address name.	string	Maximum length: 79						
srcintf <name>	One or more incoming (ingress) interfaces. Interface name.	string	Maximum length: 79						
status	Enable/disable this traffic shaping policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable traffic shaping policy.</td></tr><tr><td>disable</td><td>Disable traffic shaping policy.</td></tr></table>			Option	Description	enable	Enable traffic shaping policy.	disable	Disable traffic shaping policy.
	Option	Description							
	enable	Enable traffic shaping policy.							
disable	Disable traffic shaping policy.								
tos	ToS (Type of Service) value used for comparison.	user	Not Specified						
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified						
tos-negate	Enable negated TOS match.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TOS match negate.</td></tr><tr><td>disable</td><td>Disable TOS match negate.</td></tr></table>			Option	Description	enable	Enable TOS match negate.	disable	Disable TOS match negate.
	Option	Description							
	enable	Enable TOS match negate.							
disable	Disable TOS match negate.								
traffic-shaper	Traffic shaper to apply to traffic forwarded by the firewall policy.	string	Maximum length: 35						
traffic-shaper- reverse	Traffic shaper to apply to response traffic received by the firewall policy.	string	Maximum length: 35						
url-category <id>	IDs of one or more FortiGuard Web Filtering categories that this shaper applies traffic shaping to. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295						
users <name>	Apply this traffic shaping policy to individual users that have authenticated with the FortiGate. User name.	string	Maximum length: 79						

config firewall shaping-profile

Configure shaping profiles.

```
config firewall shaping-profile
    Description: Configure shaping profiles.
    edit <profile-name>
        set comment {var-string}
        set default-class-id {integer}
```

```

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

```

config firewall shaping-profile

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 1023
default-class-id	Default class ID to handle unclassified packets (including all local traffic).	integer	Minimum value: 0 Maximum value: 4294967295
profile-name	Shaping profile name.	string	Maximum length: 35
type	Select shaping profile type: policing / queuing.	option	-

Option	Description
<i>policing</i>	Enable policing mode.
<i>queuing</i>	Enable queuing mode.

config shaping-entries

Parameter	Description	Type	Size
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

Parameter	Description	Type	Size
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
class-id	Class ID.	integer	Minimum value: 0 Maximum value: 4294967295
guaranteed-bandwidth-percentage	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295
limit	Hard limit on the real queue size in packets.	integer	Minimum value: 5 Maximum value: 10000
max	Average queue size in packets at which RED drop probability is maximal.	integer	Minimum value: 3 Maximum value: 3000
maximum-bandwidth-percentage	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100
min	Average queue size in packets at which RED drop becomes a possibility.	integer	Minimum value: 3 Maximum value: 3000
priority	Priority.	option	-

Option	Description

<i>top</i>	Top priority.

<i>critical</i>	Critical priority.

<i>high</i>	High priority.

Parameter	Description	Type	Size
	Option	Description	
	<i>medium</i>	Medium priority.	
	<i>low</i>	Low priority.	
red-probability	Maximum probability (in percentage) for RED marking.	integer	Minimum value: 0 Maximum value: 20

config firewall sniffer

Configure sniffer.

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

```

set protocol {string}
set status [enable|disable]
set vlan {string}
set webfilter-profile {string}
set webfilter-profile-status [enable|disable]
next
end

```

config firewall sniffer

Parameter	Description	Type	Size
application-list	Name of an existing application list.	string	Maximum length: 35
application-list-status	Enable/disable application control profile.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
av-profile	Name of an existing antivirus profile.	string	Maximum length: 35
av-profile-status	Enable/disable antivirus profile.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35
dlp-sensor-status	Enable/disable DLP sensor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
dsri	Enable/disable DSRI.	option	-
	Option	Description	
	<i>enable</i>	Enable DSRI.	
	<i>disable</i>	Disable DSRI.	

Parameter	Description	Type	Size						
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35						
emailfilter-profile-status	Enable/disable emailfilter.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
host	Hosts to filter for in sniffer traffic (Format examples: 1.1.1.1, 2.2.2.0/24, 3.3.3.3/255.255.255.0, 4.4.4.0-4.4.4.240).	string	Maximum length: 63						
id	Sniffer ID.	integer	Minimum value: 0 Maximum value: 9999						
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35						
ips-dos-status	Enable/disable IPS DoS anomaly detection.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35						
ips-sensor-status	Enable/disable IPS sensor.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
ipv6	Enable/disable sniffing IPv6 packets.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer for IPv6 packets.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer for IPv6 packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer for IPv6 packets.	<i>disable</i>	Disable sniffer for IPv6 packets.		
Option	Description								
<i>enable</i>	Enable sniffer for IPv6 packets.								
<i>disable</i>	Disable sniffer for IPv6 packets.								

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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td>utm</td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td>disable</td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	all	Log all sessions accepted or denied by this policy.	utm	Log traffic that has a security profile applied to it.	disable	Disable all logging for this policy.		
Option	Description										
all	Log all sessions accepted or denied by this policy.										
utm	Log traffic that has a security profile applied to it.										
disable	Disable all logging for this policy.										
max-packet-count	Maximum packet count (1 - 1000000, default = 4000).	integer	Minimum value: 1 Maximum value: 1000000 **								
non-ip	Enable/disable sniffing non-IP packets.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer for non-IP packets.</td></tr><tr><td>disable</td><td>Disable sniffer for non-IP packets.</td></tr></table>	Option	Description	enable	Enable sniffer for non-IP packets.	disable	Disable sniffer for non-IP packets.				
Option	Description										
enable	Enable sniffer for non-IP packets.										
disable	Disable sniffer for non-IP packets.										
port	Ports to sniff (Format examples: 10, :20, 30:40, 50-, 100-200).	string	Maximum length: 63								
protocol	Integer value for the protocol type as defined by IANA (0 - 255).	string	Maximum length: 63								
status	Enable/disable the active status of the sniffer.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer status.</td></tr><tr><td>disable</td><td>Disable sniffer status.</td></tr></table>	Option	Description	enable	Enable sniffer status.	disable	Disable sniffer status.				
Option	Description										
enable	Enable sniffer status.										
disable	Disable sniffer status.										
vlan	List of VLANs to sniff.	string	Maximum length: 63								
webfilter-profile	Name of an existing web filter profile.	string	Maximum length: 35								
webfilter-profile-status	Enable/disable web filter profile.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.				
Option	Description										
enable	Enable setting.										
disable	Disable setting.										

** Values may differ between models.

config anomaly

Parameter	Description	Type	Size						
action	Action taken when the threshold is reached.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Allow traffic but record a log message if logging is enabled.</td></tr><tr><td>block</td><td>Block traffic if this anomaly is found.</td></tr></table>	Option	Description	pass	Allow traffic but record a log message if logging is enabled.	block	Block traffic if this anomaly is found.		
Option	Description								
pass	Allow traffic but record a log message if logging is enabled.								
block	Block traffic if this anomaly is found.								
log	Enable/disable anomaly logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable anomaly logging.</td></tr><tr><td>disable</td><td>Disable anomaly logging.</td></tr></table>	Option	Description	enable	Enable anomaly logging.	disable	Disable anomaly logging.		
Option	Description								
enable	Enable anomaly logging.								
disable	Disable anomaly logging.								
name	Anomaly name.	string	Maximum length: 63						
quarantine	Quarantine method.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Quarantine is disabled.</td></tr><tr><td>attacker</td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	none	Quarantine is disabled.	attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
Option	Description								
none	Quarantine is disabled.								
attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.								
quarantine-expiry	Duration of quarantine. (Format ####d##h##m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified						
quarantine-log	Enable/disable quarantine logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable quarantine logging.</td></tr><tr><td>enable</td><td>Enable quarantine logging.</td></tr></table>	Option	Description	disable	Disable quarantine logging.	enable	Enable quarantine logging.		
Option	Description								
disable	Disable quarantine logging.								
enable	Enable quarantine logging.								
status	Enable/disable this anomaly.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this status.</td></tr><tr><td>enable</td><td>Enable this status.</td></tr></table>	Option	Description	disable	Disable this status.	enable	Enable this status.		
Option	Description								
disable	Disable this status.								
enable	Enable this status.								

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 (1 - 2147483647, default = 1000). Note that each anomaly has a different threshold value assigned to it. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295

config firewall ssh host-key

SSH proxy host public keys.

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

config firewall ssh host-key

Parameter	Description	Type	Size
hostname	Hostname of the SSH server.	string	Maximum length: 255
ip	IP address of the SSH server.	ipv4-address-any	Not Specified
name	SSH public key name.	string	Maximum length: 35
nid	Set the nid of the ECDSA key.	option	-
	Option	Description	
	256	The NID is ecdsa-sha2-nistp256.	

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>384</td><td>The NID is ecdsa-sha2-nistp384.</td></tr><tr><td>521</td><td>The NID is ecdsa-sha2-nistp521.</td></tr></table>	Option	Description	384	The NID is ecdsa-sha2-nistp384.	521	The NID is ecdsa-sha2-nistp521.														
	Option	Description																			
	384	The NID is ecdsa-sha2-nistp384.																			
521	The NID is ecdsa-sha2-nistp521.																				
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295																		
public-key	SSH public key.	var-string	Maximum length: 32768																		
status	Set the trust status of the public key.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>trusted</td><td>The public key is trusted.</td></tr><tr><td>revoked</td><td>The public key is revoked.</td></tr></table>	Option	Description	trusted	The public key is trusted.	revoked	The public key is revoked.														
	Option	Description																			
	trusted	The public key is trusted.																			
revoked	The public key is revoked.																				
type	Set the type of the public key.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>RSA</td><td>The type of the public key is RSA.</td></tr><tr><td>DSA</td><td>The type of the public key is DSA.</td></tr><tr><td>ECDSA</td><td>The type of the public key is ECDSA.</td></tr><tr><td>ED25519</td><td>The type of the public key is ED25519.</td></tr><tr><td>RSA-CA</td><td>The type of the public key is from RSA CA.</td></tr><tr><td>DSA-CA</td><td>The type of the public key is from DSA CA.</td></tr><tr><td>ECDSA-CA</td><td>The type of the public key is from ECDSA CA.</td></tr><tr><td>ED25519-CA</td><td>The type of the public key is from ED25519 CA.</td></tr></table>	Option	Description	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.	RSA-CA	The type of the public key is from RSA CA.	DSA-CA	The type of the public key is from DSA CA.	ECDSA-CA	The type of the public key is from ECDSA CA.	ED25519-CA	The type of the public key is from ED25519 CA.		
	Option	Description																			
	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.																			
	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.																				

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
name	SSH proxy local CA name.	string	Maximum length: 35
password	Password for SSH private key.	password	Not Specified
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified
public-key	SSH proxy public key.	user	Not Specified
source	SSH proxy local CA source type.	option	-

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

config firewall ssh local-key

SSH proxy local keys.

```
config firewall ssh local-key
  Description: SSH proxy local keys.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end
```

config firewall ssh local-key

Parameter	Description	Type	Size
name	SSH proxy local key name.	string	Maximum length: 35
password	Password for SSH private key.	password	Not Specified

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

config firewall ssh setting

SSH proxy settings.

```
config firewall ssh setting
    Description: SSH proxy settings.
    set caname {string}
    set host-trusted-checking [enable|disable]
    set hostkey-dsa1024 {string}
    set hostkey-ecdsa256 {string}
    set hostkey-ecdsa384 {string}
    set hostkey-ecdsa521 {string}
    set hostkey-ed25519 {string}
    set hostkey-rsa2048 {string}
    set untrusted-caname {string}
end
```

config firewall ssh setting

Parameter	Description	Type	Size
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35
host-trusted-checking	Enable/disable host trusted checking.	option	-
	Option	Description	
	<i>enable</i>	Enable host key trusted checking.	
	<i>disable</i>	Disable host key trusted checking.	
hostkey-dsa1024	DSA certificate used by SSH proxy.	string	Maximum length: 35

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

config firewall ssl setting

SSL proxy settings.

```
config firewall ssl setting
    Description: SSL proxy settings.
    set abbreviate-handshake [enable|disable]
    set cert-cache-capacity {integer}
    set cert-cache-timeout {integer}
    set kxp-queue-threshold {integer}
    set no-matching-cipher-action [bypass|drop]
    set proxy-connect-timeout {integer}
    set session-cache-capacity {integer}
    set session-cache-timeout {integer}
    set ssl-dh-bits [768|1024|...]
    set ssl-queue-threshold {integer}
    set ssl-send-empty-frags [enable|disable]
end
```

config firewall ssl setting

Parameter	Description	Type	Size
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-
	Option	Description	
	<i>enable</i>	Enable use of SSL abbreviated handshake.	
	<i>disable</i>	Disable use of SSL abbreviated handshake.	

Parameter	Description	Type	Size
cert-cache-capacity	Maximum capacity of the host certificate cache (0 - 500, default = 200).	integer	Minimum value: 0 Maximum value: 500
cert-cache-timeout	Time limit to keep certificate cache (1 - 120 min, default = 10).	integer	Minimum value: 1 Maximum value: 120
kxp-queue-threshold *	Maximum length of the CP KXP queue. When the queue becomes full, the proxy switches cipher functions to the main CPU (0 - 512, default = 16).	integer	Minimum value: 0 Maximum value: 512
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-

Option	Description

<i>bypass</i>	Bypass connection.

<i>drop</i>	Drop connection.

proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process (1 - 60 sec, default = 30).	integer	Minimum value: 1 Maximum value: 60
session-cache-capacity	Capacity of the SSL session cache (--Obsolete--) (1 - 1000, default = 500).	integer	Minimum value: 0 Maximum value: 1000
session-cache-timeout	Time limit to keep SSL session state (1 - 60 min, default = 20).	integer	Minimum value: 1 Maximum value: 60
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-

Option	Description

<i>768</i>	768-bit Diffie-Hellman prime.

<i>1024</i>	1024-bit Diffie-Hellman prime.

<i>1536</i>	1536-bit Diffie-Hellman prime.

<i>2048</i>	2048-bit Diffie-Hellman prime.

Parameter	Description	Type	Size
ssl-queue-threshold *	Maximum length of the CP SSL queue. When the queue becomes full, the proxy switches cipher functions to the main CPU (0 - 512, default = 32).	integer	Minimum value: 0 Maximum value: 512
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
<i>enable</i>	Send empty fragments.
<i>disable</i>	Do not send empty fragments.

* This parameter may not exist in some models.

config firewall ssl-server

Configure SSL servers.

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

config firewall ssl-server

Parameter	Description	Type	Size
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Add X-Forwarded-Proto header.
<i>disable</i>	Do not add X-Forwarded-Proto header.

ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified
mapped-port	Mapped server service port (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535
name	Server name.	string	Maximum length: 35
port	Server service port (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-

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

ssl-cert	Name of certificate for SSL connections to this server (default = "Fortinet_CA_SSL").	string	Maximum length: 35
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-

Option	Description
<i>allow</i>	Allow a SSL client to renegotiate.
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.

ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-

Parameter	Description	Type	Size	
	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-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.		
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.		
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.		
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.		
url-rewrite	Enable/disable rewriting the URL.	option	-	
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

```
config firewall ssl-ssh-profile
  Description: Configure SSL/SSH protocol options.
  edit <name>
    set block-blacklisted-certificates [disable|enable]
    set caname {string}
    set comment {var-string}
    config ftps
      Description: Configure FTPS options.
      set client-cert-request [bypass|inspect|...]
      set invalid-server-cert [allow|block]
      set ports {integer}
      set sni-server-cert-check [enable|strict|...]
      set status [disable|deep-inspection]
      set unsupported-ssl [bypass|inspect|...]
      set untrusted-server-cert [allow|block|...]
    end
    config https
      Description: Configure HTTPS options.
      set client-cert-request [bypass|inspect|...]
      set invalid-server-cert [allow|block]
      set ports {integer}
      set sni-server-cert-check [enable|strict|...]
      set status [disable|certificate-inspection|...]
      set unsupported-ssl [bypass|inspect|...]
      set untrusted-server-cert [allow|block|...]
    end
    config imaps
      Description: Configure IMAPS options.
      set client-cert-request [bypass|inspect|...]
      set invalid-server-cert [allow|block]
      set ports {integer}
      set sni-server-cert-check [enable|strict|...]
      set status [disable|deep-inspection]
      set unsupported-ssl [bypass|inspect|...]
      set untrusted-server-cert [allow|block|...]
    end
    set mapi-over-https [enable|disable]
    config pop3s
      Description: Configure POP3S options.
      set client-cert-request [bypass|inspect|...]
      set invalid-server-cert [allow|block]
      set ports {integer}
      set sni-server-cert-check [enable|strict|...]
      set status [disable|deep-inspection]
      set unsupported-ssl [bypass|inspect|...]
      set untrusted-server-cert [allow|block|...]
    end
    set rpc-over-https [enable|disable]
    set server-cert {string}
    set server-cert-mode [re-sign|replace]
    config smtps
```



```

        Description: Configure SMTPS options.
        set client-cert-request [bypass|inspect|...]
        set invalid-server-cert [allow|block]
        set ports {integer}
        set sni-server-cert-check [enable|strict|...]
        set status [disable|deep-inspection]
        set unsupported-ssl [bypass|inspect|...]
        set untrusted-server-cert [allow|block|...]
    end
    config ssh
        Description: Configure SSH options.
        set inspect-all [disable|deep-inspection]
        set ports {integer}
        set ssh-algorithm [compatible|high-encryption]
        set ssh-tun-policy-check [disable|enable]
        set status [disable|deep-inspection]
        set unsupported-version [bypass|block]
    end
    config ssl
        Description: Configure SSL options.
        set client-cert-request [bypass|inspect|...]
        set inspect-all [disable|certificate-inspection|...]
        set invalid-server-cert [allow|block]
        set sni-server-cert-check [enable|strict|...]
        set unsupported-ssl [bypass|inspect|...]
        set untrusted-server-cert [allow|block|...]
    end
    set ssl-anomalies-log [disable|enable]
    config ssl-exempt
        Description: Servers to exempt from SSL inspection.
        edit <id>
            set address {string}
            set address6 {string}
            set fortiguard-category {integer}
            set regex {string}
            set type [fortiguard-category|address|...]
            set wildcard-fqdn {string}
        next
    end
    set ssl-exemptions-log [disable|enable]
    config ssl-server
        Description: SSL servers.
        edit <id>
            set ftps-client-cert-request [bypass|inspect|...]
            set https-client-cert-request [bypass|inspect|...]
            set imaps-client-cert-request [bypass|inspect|...]
            set ip {ipv4-address-any}
            set pop3s-client-cert-request [bypass|inspect|...]
            set smtps-client-cert-request [bypass|inspect|...]
            set ssl-other-client-cert-request [bypass|inspect|...]
        next
    end
    set untrusted-caname {string}
    set use-ssl-server [disable|enable]
    set whitelist [enable|disable]
next

```

end

config firewall ssl-ssh-profile

Parameter	Description	Type	Size						
block-blacklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blacklist.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiGuard certificate blacklist.</td></tr><tr><td><i>enable</i></td><td>Enable FortiGuard certificate blacklist.</td></tr></table>			Option	Description	<i>disable</i>	Disable FortiGuard certificate blacklist.	<i>enable</i>	Enable FortiGuard certificate blacklist.
Option	Description								
<i>disable</i>	Disable FortiGuard certificate blacklist.								
<i>enable</i>	Enable FortiGuard certificate blacklist.								
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35						
comment	Optional comments.	var-string	Maximum length: 255						
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of MAPI over HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of MAPI over HTTPS.</td></tr></table>			Option	Description	<i>enable</i>	Enable inspection of MAPI over HTTPS.	<i>disable</i>	Disable inspection of MAPI over HTTPS.
Option	Description								
<i>enable</i>	Enable inspection of MAPI over HTTPS.								
<i>disable</i>	Disable inspection of MAPI over HTTPS.								
name	Name.	string	Maximum length: 35						
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of RPC over HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of RPC over HTTPS.</td></tr></table>			Option	Description	<i>enable</i>	Enable inspection of RPC over HTTPS.	<i>disable</i>	Disable inspection of RPC over HTTPS.
Option	Description								
<i>enable</i>	Enable inspection of RPC over HTTPS.								
<i>disable</i>	Disable inspection of RPC over HTTPS.								
server-cert	Certificate used by SSL Inspection to replace server certificate.	string	Maximum length: 35						
server-cert-mode	Re-sign or replace the server's certificate.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>re-sign</i></td><td>Multiple clients connecting to multiple servers.</td></tr><tr><td><i>replace</i></td><td>Protect an SSL server.</td></tr></table>			Option	Description	<i>re-sign</i>	Multiple clients connecting to multiple servers.	<i>replace</i>	Protect an SSL server.
Option	Description								
<i>re-sign</i>	Multiple clients connecting to multiple servers.								
<i>replace</i>	Protect an SSL server.								

Parameter	Description	Type	Size						
ssl-anomalies-log	Enable/disable logging SSL anomalies.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging SSL anomalies.</td></tr><tr><td><i>enable</i></td><td>Enable logging SSL anomalies.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging SSL anomalies.	<i>enable</i>	Enable logging SSL anomalies.		
Option	Description								
<i>disable</i>	Disable logging SSL anomalies.								
<i>enable</i>	Enable logging SSL anomalies.								
ssl-exemptions-log	Enable/disable logging SSL exemptions.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging SSL exemptions.</td></tr><tr><td><i>enable</i></td><td>Enable logging SSL exemptions.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging SSL exemptions.	<i>enable</i>	Enable logging SSL exemptions.		
Option	Description								
<i>disable</i>	Disable logging SSL exemptions.								
<i>enable</i>	Enable logging SSL exemptions.								
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35						
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Don't use SSL server configuration.</td></tr><tr><td><i>enable</i></td><td>Use SSL server configuration.</td></tr></table>	Option	Description	<i>disable</i>	Don't use SSL server configuration.	<i>enable</i>	Use SSL server configuration.		
Option	Description								
<i>disable</i>	Don't use SSL server configuration.								
<i>enable</i>	Use SSL server configuration.								
whitelist	Enable/disable exempting servers by FortiGuard whitelist.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

config ftps

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								
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the invalid server certificate.</td></tr><tr><td><i>block</i></td><td>Block the connection when an invalid server certificate is detected.</td></tr></table>	Option	Description	<i>allow</i>	Allow the invalid server certificate.	<i>block</i>	Block the connection when an invalid server certificate is detected.				
Option	Description										
<i>allow</i>	Allow the invalid server certificate.										
<i>block</i>	Block the connection when an invalid server certificate is detected.										
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535								
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
Option	Description										
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.										
status	Configure protocol inspection status.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.				
Option	Description										
<i>disable</i>	Disable.										
<i>deep-inspection</i>	Full SSL inspection.										
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.		
Option	Description										
<i>bypass</i>	Bypass the session.										
<i>inspect</i>	Inspect the session.										
<i>block</i>	Block the session.										
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>allow</i>	Allow the untrusted server certificate.	
	<i>block</i>	Block the connection when an untrusted server certificate is detected.	
	<i>ignore</i>	Always take the server certificate as trusted.	

config https

Parameter	Description	Type	Size
client-cert-request	Action based on client certificate request.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-
	Option	Description	
	<i>allow</i>	Allow the invalid server certificate.	
	<i>block</i>	Block the connection when an invalid server certificate is detected.	
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535
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	
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	

Parameter	Description	Type	Size
status	Configure protocol inspection status.	option	-
	Option	Description	
	<i>disable</i>	Disable.	
	<i>certificate-inspection</i>	Inspect SSL handshake only.	
	<i>deep-inspection</i>	Full SSL inspection.	
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-
	Option	Description	
	<i>allow</i>	Allow the untrusted server certificate.	
	<i>block</i>	Block the connection when an untrusted server certificate is detected.	
	<i>ignore</i>	Always take the server certificate as trusted.	

config imaps

Parameter	Description	Type	Size
client-cert-request	Action based on client certificate request.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the invalid server certificate.</td></tr><tr><td><i>block</i></td><td>Block the connection when an invalid server certificate is detected.</td></tr></table>	Option	Description	<i>allow</i>	Allow the invalid server certificate.	<i>block</i>	Block the connection when an invalid server certificate is detected.				
Option	Description										
<i>allow</i>	Allow the invalid server certificate.										
<i>block</i>	Block the connection when an invalid server certificate is detected.										
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535								
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
Option	Description										
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.										
status	Configure protocol inspection status.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.				
Option	Description										
<i>disable</i>	Disable.										
<i>deep-inspection</i>	Full SSL inspection.										
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.		
Option	Description										
<i>bypass</i>	Bypass the session.										
<i>inspect</i>	Inspect the session.										
<i>block</i>	Block the session.										
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the untrusted server certificate.</td></tr></table>	Option	Description	<i>allow</i>	Allow the untrusted server certificate.						
Option	Description										
<i>allow</i>	Allow the untrusted server certificate.										

Parameter	Description	Type	Size
	Option	Description	
	<i>block</i>	Block the connection when an untrusted server certificate is detected.	
	<i>ignore</i>	Always take the server certificate as trusted.	

config pop3s

Parameter	Description	Type	Size
client-cert-request	Action based on client certificate request.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-
	Option	Description	
	<i>allow</i>	Allow the invalid server certificate.	
	<i>block</i>	Block the connection when an invalid server certificate is detected.	
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535
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	
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	
status	Configure protocol inspection status.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.				
	Option	Description									
	<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.										
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.		
	Option	Description									
	<i>bypass</i>	Bypass the session.									
	<i>inspect</i>	Inspect the session.									
<i>block</i>	Block the session.										
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the untrusted server certificate.</td></tr><tr><td><i>block</i></td><td>Block the connection when an untrusted server certificate is detected.</td></tr><tr><td><i>ignore</i></td><td>Always take the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the untrusted server certificate.	<i>block</i>	Block the connection when an untrusted server certificate is detected.	<i>ignore</i>	Always take the server certificate as trusted.		
	Option	Description									
	<i>allow</i>	Allow the untrusted server certificate.									
<i>block</i>	Block the connection when an untrusted server certificate is detected.										
<i>ignore</i>	Always take the server certificate as trusted.										

config smtps

Parameter	Description	Type	Size								
client-cert-request	Action based on client certificate request.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.		
Option	Description										
bypass	Bypass the session.										
inspect	Inspect the session.										
block	Block the session.										
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the invalid server certificate.</td></tr><tr><td>block</td><td>Block the connection when an invalid server certificate is detected.</td></tr></table>	Option	Description	allow	Allow the invalid server certificate.	block	Block the connection when an invalid server certificate is detected.				
Option	Description										
allow	Allow the invalid server certificate.										
block	Block the connection when an invalid server certificate is detected.										

Parameter	Description	Type	Size
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535
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
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

status	Configure protocol inspection status.	option	-

Option	Description
<i>disable</i>	Disable.
<i>deep-inspection</i>	Full SSL inspection.

unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-

Option	Description
<i>bypass</i>	Bypass the session.
<i>inspect</i>	Inspect the session.
<i>block</i>	Block the session.

untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-

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

config ssh

Parameter	Description	Type	Size						
inspect-all	Level of SSL inspection.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.		
Option	Description								
<i>disable</i>	Disable.								
<i>deep-inspection</i>	Full SSL inspection.								
ports	Ports to use for scanning (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535						
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>compatible</i></td><td>Allow a broader set of encryption algorithms for best compatibility.</td></tr><tr><td><i>high-encryption</i></td><td>Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.</td></tr></table>	Option	Description	<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.	<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.		
Option	Description								
<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.								
<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.								
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSH tunnel policy check.</td></tr><tr><td><i>enable</i></td><td>Enable SSH tunnel policy check.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSH tunnel policy check.	<i>enable</i>	Enable SSH tunnel policy check.		
Option	Description								
<i>disable</i>	Disable SSH tunnel policy check.								
<i>enable</i>	Enable SSH tunnel policy check.								
status	Configure protocol inspection status.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.		
Option	Description								
<i>disable</i>	Disable.								
<i>deep-inspection</i>	Full SSL inspection.								
unsupported-version	Action based on SSH version being unsupported.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>block</i>	Block the session.		
Option	Description								
<i>bypass</i>	Bypass the session.								
<i>block</i>	Block the session.								

config ssl

Parameter	Description	Type	Size								
client-cert-request	Action based on client certificate request.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.		
Option	Description										
bypass	Bypass the session.										
inspect	Inspect the session.										
block	Block the session.										
inspect-all	Level of SSL inspection.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>certificate-inspection</td><td>Inspect SSL handshake only.</td></tr><tr><td>deep-inspection</td><td>Full SSL inspection.</td></tr></table>	Option	Description	disable	Disable.	certificate-inspection	Inspect SSL handshake only.	deep-inspection	Full SSL inspection.		
Option	Description										
disable	Disable.										
certificate-inspection	Inspect SSL handshake only.										
deep-inspection	Full SSL inspection.										
invalid-server-cert	Allow or block the invalid SSL session server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the invalid server certificate.</td></tr><tr><td>block</td><td>Block the connection when an invalid server certificate is detected.</td></tr></table>	Option	Description	allow	Allow the invalid server certificate.	block	Block the connection when an invalid server certificate is detected.				
Option	Description										
allow	Allow the invalid server certificate.										
block	Block the connection when an invalid server certificate is detected.										
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td>strict</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td>disable</td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
Option	Description										
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.										
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.										
unsupported-ssl	Action based on the SSL encryption used being unsupported.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
untrusted-server-cert	Allow, ignore, or block the untrusted SSL session server certificate.	option	-
	Option	Description	
	<i>allow</i>	Allow the untrusted server certificate.	
	<i>block</i>	Block the connection when an untrusted server certificate is detected.	
	<i>ignore</i>	Always take the server certificate as trusted.	

config ssl-exempt

Parameter	Description	Type	Size
address	IPv4 address object.	string	Maximum length: 79
address6	IPv6 address object.	string	Maximum length: 79
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255
id	ID number.	integer	Minimum value: 0 Maximum value: 512
regex	Exempt servers by regular expression.	string	Maximum length: 255
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-
	Option	Description	
	<i>fortiguard-category</i>	FortiGuard category.	
	<i>address</i>	Firewall IPv4 address.	

Parameter	Description	Type	Size
	Option	Description	
	<i>address6</i>	Firewall IPv6 address.	
	<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.	
	<i>regex</i>	Regular expression FQDN.	
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79

config ssl-server

Parameter	Description	Type	Size
ftps-client-cert-request	Action based on client certificate request during the FTPS handshake.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
https-client-cert-request	Action based on client certificate request during the HTTPS handshake.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295
imaps-client-cert-request	Action based on client certificate request during the IMAPS handshake.	option	-
	Option	Description	
	<i>bypass</i>	Bypass the session.	
	<i>inspect</i>	Inspect the session.	
	<i>block</i>	Block the session.	

Parameter	Description	Type	Size								
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified								
pop3s-client-cert-request	Action based on client certificate request during the POP3S handshake.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.		
Option	Description										
bypass	Bypass the session.										
inspect	Inspect the session.										
block	Block the session.										
smtps-client-cert-request	Action based on client certificate request during the SMTPS handshake.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.		
Option	Description										
bypass	Bypass the session.										
inspect	Inspect the session.										
block	Block the session.										
ssl-other-client-cert-request	Action based on client certificate request during an SSL protocol handshake.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.		
Option	Description										
bypass	Bypass the session.										
inspect	Inspect the session.										
block	Block the session.										

config firewall traffic-class

Configure names for shaping classes.

```
config firewall traffic-class
    Description: Configure names for shaping classes.
    edit <class-id>
        set class-name {string}
    next
end
```

config firewall traffic-class

Parameter	Description	Type	Size
class-id	Class ID to be named.	integer	Minimum value: 2 Maximum value: 31
class-name	Define the name for this class-id.	string	Maximum length: 35

config firewall ttl-policy

Configure TTL policies.

```
config firewall ttl-policy
  Description: Configure TTL policies.
  edit <id>
    set action [accept|deny]
    set schedule {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set status [enable|disable]
    set ttl {user}
  next
end
```

config firewall ttl-policy

Parameter	Description	Type	Size
action	Action to be performed on traffic matching this policy (default = deny).	option	-
	Option	Description	
	<i>accept</i>	Allow traffic matching this policy.	
	<i>deny</i>	Deny or block traffic matching this policy.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
schedule	Schedule object from available options.	string	Maximum length: 35

Parameter	Description	Type	Size						
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79						
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79						
srcintf	Source interface name from available interfaces.	string	Maximum length: 35						
status	Enable/disable this TTL policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this TTL policy.</td></tr><tr><td>disable</td><td>Disable this TTL policy.</td></tr></table>			Option	Description	enable	Enable this TTL policy.	disable	Disable this TTL policy.
	Option	Description							
	enable	Enable this TTL policy.							
disable	Disable this TTL policy.								
ttl	Value/range to match against the packet's Time to Live value (format: ttl[- ttl_high], 1 - 255).	user	Not Specified						

config firewall vip

Configure virtual IP for IPv4.

```
config firewall vip
  Description: Configure virtual IP for IPv4.
  edit <name>
    set arp-reply [disable|enable]
    set color {integer}
    set comment {var-string}
    set dns-mapping-ttl {integer}
    set extaddr <name1>, <name2>, ...
    set extintf {string}
    set extip {user}
    set extport {user}
    set gratuitous-arp-interval {integer}
    set http-cookie-age {integer}
    set http-cookie-domain {string}
    set http-cookie-domain-from-host [disable|enable]
    set http-cookie-generation {integer}
    set http-cookie-path {string}
    set http-cookie-share [disable|same-ip]
    set http-ip-header [enable|disable]
    set http-ip-header-name {string}
    set http-multiplex [enable|disable]
    set http-redirect [enable|disable]
    set https-cookie-secure [disable|enable]
    set id {integer}
    set ldb-method [static|round-robin|...]
    set mapped-addr {string}
```

```

set mappedip <range1>, <range2>, ...
set mappedport {user}
set max-embryonic-connections {integer}
set monitor <name1>, <name2>, ...
set nat-source-vip [disable|enable]
set outlook-web-access [disable|enable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set portmapping-type [1-to-1|m-to-n]
set protocol [tcp|udp|...]
config realservers
    Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
    edit <id>
        set client-ip {user}
        set healthcheck [disable|enable|...]
        set holddown-interval {integer}
        set http-host {string}
        set ip {ipv4-address-any}
        set max-connections {integer}
        set monitor {string}
        set port {integer}
        set status [active|standby|...]
        set weight {integer}
    next
end
set server-type [http|https|...]
set service <name1>, <name2>, ...
set src-filter <range1>, <range2>, ...
set srcintf-filter <interface-name1>, <interface-name2>, ...
set ssl-algorithm [high|medium|...]
set ssl-certificate {string}
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-client-fallback [disable|enable]
set ssl-client-rekey-count {integer}
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-max {integer}
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-type [disable|time|...]
set ssl-dh-bits [768|1024|...]
set ssl-hpkip [disable|enable|...]
set ssl-hpkip-age {integer}
set ssl-hpkip-backup {string}
set ssl-hpkip-include-subdomains [disable|enable]
set ssl-hpkip-primary {string}
set ssl-hpkip-report-uri {var-string}
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]

```

```

set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-mode [half|full]
set ssl-pfs [require|deny|...]
set ssl-send-empty-frags [enable|disable]
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-session-state-max {integer}
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-type [disable|time|...]
set type [static-nat|load-balance|...]
set uuid {uuid}
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
next
end

```

config firewall vip

Parameter	Description	Type	Size
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
dns-mapping-ttl	DNS mapping TTL (Set to zero to use TTL in DNS response, default = 0).	integer	Minimum value: 0 Maximum value: 604800

Parameter	Description	Type	Size
extaddr <name>	External FQDN address name. Address name.	string	Maximum length: 79
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified
gratuitous-arp-interval	Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to enable.	integer	Minimum value: 5 Maximum value: 8640000
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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-

Option	Description
<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.

http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35
http-cookie-share	Control sharing of cookies across virtual servers. same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Only allow HTTP cookie to match this virtual server.</td></tr><tr><td><i>same-ip</i></td><td>Allow HTTP cookie to match any virtual server with same IP.</td></tr></table>	Option	Description	<i>disable</i>	Only allow HTTP cookie to match this virtual server.	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.		
Option	Description								
<i>disable</i>	Only allow HTTP cookie to match this virtual server.								
<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.								
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding HTTP header.</td></tr><tr><td><i>disable</i></td><td>Disable adding HTTP header.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding HTTP header.	<i>disable</i>	Disable adding HTTP header.		
Option	Description								
<i>enable</i>	Enable adding HTTP header.								
<i>disable</i>	Disable adding HTTP header.								
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35						
http-multiplex	Enable/disable HTTP multiplexing.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP session multiplexing.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP session multiplexing.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP session multiplexing.	<i>disable</i>	Disable HTTP session multiplexing.		
Option	Description								
<i>enable</i>	Enable HTTP session multiplexing.								
<i>disable</i>	Disable HTTP session multiplexing.								
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirection of HTTP to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirection of HTTP to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.		
Option	Description								
<i>enable</i>	Enable redirection of HTTP to HTTPS.								
<i>disable</i>	Disable redirection of HTTP to HTTPS.								
https-cookie-secure *	Enable/disable verification that inserted HTTPS cookies are secure.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
Option	Description								
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.								
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.								
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535						

Parameter	Description	Type	Size
ldb-method	Method used to distribute sessions to real servers.	option	-

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

mapped-addr	Mapped FQDN address name.	string	Maximum length: 79
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79
name	Virtual IP name.	string	Maximum length: 79
nat-source-vip	Enable/disable forcing the source NAT mapped IP to the external IP for all traffic.	option	-

Option	Description
<i>disable</i>	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.
<i>enable</i>	Force the source NAT mapped IP to the external IP for all traffic.

Parameter	Description	Type	Size										
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Outlook Web Access support.</td></tr><tr><td><i>enable</i></td><td>Enable Outlook Web Access support.</td></tr></table>	Option	Description	<i>disable</i>	Disable Outlook Web Access support.	<i>enable</i>	Enable Outlook Web Access support.						
Option	Description												
<i>disable</i>	Disable Outlook Web Access support.												
<i>enable</i>	Enable Outlook Web Access support.												
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr><tr><td><i>ssl-session-id</i></td><td>SSL session ID.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.	<i>ssl-session-id</i>	SSL session ID.				
Option	Description												
<i>none</i>	None.												
<i>http-cookie</i>	HTTP cookie.												
<i>ssl-session-id</i>	SSL session ID.												
portforward	Enable/disable port forwarding.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable port forward.</td></tr><tr><td><i>enable</i></td><td>Enable port forward.</td></tr></table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable port forward.						
Option	Description												
<i>disable</i>	Disable port forward.												
<i>enable</i>	Enable port forward.												
portmapping-type	Port mapping type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1-to-1</i></td><td>One to one.</td></tr><tr><td><i>m-to-n</i></td><td>Many to many.</td></tr></table>	Option	Description	<i>1-to-1</i>	One to one.	<i>m-to-n</i>	Many to many.						
Option	Description												
<i>1-to-1</i>	One to one.												
<i>m-to-n</i>	Many to many.												
protocol	Protocol to use when forwarding packets.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>sctp</i></td><td>SCTP.</td></tr><tr><td><i>icmp</i></td><td>ICMP.</td></tr></table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.	<i>icmp</i>	ICMP.		
Option	Description												
<i>tcp</i>	TCP.												
<i>udp</i>	UDP.												
<i>sctp</i>	SCTP.												
<i>icmp</i>	ICMP.												
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-										

Parameter	Description	Type	Size																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>https</i></td><td>HTTPS</td></tr><tr><td><i>imaps</i></td><td>IMAPS</td></tr><tr><td><i>pop3s</i></td><td>POP3S</td></tr><tr><td><i>smtps</i></td><td>SMTPS</td></tr><tr><td><i>ssl</i></td><td>SSL</td></tr><tr><td><i>tcp</i></td><td>TCP</td></tr><tr><td><i>udp</i></td><td>UDP</td></tr><tr><td><i>ip</i></td><td>IP</td></tr></table>	Option	Description	<i>http</i>	HTTP	<i>https</i>	HTTPS	<i>imaps</i>	IMAPS	<i>pop3s</i>	POP3S	<i>smtps</i>	SMTPS	<i>ssl</i>	SSL	<i>tcp</i>	TCP	<i>udp</i>	UDP	<i>ip</i>	IP		
	Option	Description																					
	<i>http</i>	HTTP																					
	<i>https</i>	HTTPS																					
	<i>imaps</i>	IMAPS																					
	<i>pop3s</i>	POP3S																					
	<i>smtps</i>	SMTPS																					
	<i>ssl</i>	SSL																					
	<i>tcp</i>	TCP																					
	<i>udp</i>	UDP																					
<i>ip</i>	IP																						
service <name>	Service name. Service name.	string	Maximum length: 79																				
src-filter <range>	Source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y.y). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79																				
srcintf-filter <interface-name>	Interfaces to which the VIP applies. Separate the names with spaces. Interface name.	string	Maximum length: 79																				
ssl-algorithm *	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td><i>custom</i></td><td>Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	<i>custom</i>	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.												
	Option	Description																					
	<i>high</i>	High encryption. Allow only AES and ChaCha.																					
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																					
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																					
<i>custom</i>	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.																						
ssl-certificate *	The name of the SSL certificate to use for SSL acceleration.	string	Maximum length: 35																				
ssl-client-fallback *	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-																				

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.						
	Option	Description											
	<i>disable</i>	Disable.											
<i>enable</i>	Enable.												
ssl-client-rekey-count *	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576										
ssl-client-renegotiation *	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any client initiated SSL re-negotiation attempt.</td></tr><tr><td><i>secure</i></td><td>Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.	<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.				
	Option	Description											
	<i>allow</i>	Allow a SSL client to renegotiate.											
	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.											
<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.												
ssl-client-session-state-max *	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000										
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-type *	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not keep session states.</td></tr><tr><td><i>time</i></td><td>Expire session states after this many minutes.</td></tr><tr><td><i>count</i></td><td>Expire session states when this maximum is reached.</td></tr><tr><td><i>both</i></td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.		
	Option	Description											
	<i>disable</i>	Do not keep session states.											
	<i>time</i>	Expire session states after this many minutes.											
	<i>count</i>	Expire session states when this maximum is reached.											
<i>both</i>	Expire session states based on time or count, whichever occurs first.												
ssl-dh-bits *	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-										

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.		
	Option	Description															
	768	768-bit Diffie-Hellman prime.															
	1024	1024-bit Diffie-Hellman prime.															
	1536	1536-bit Diffie-Hellman prime.															
	2048	2048-bit Diffie-Hellman prime.															
	3072	3072-bit Diffie-Hellman prime.															
4096	4096-bit Diffie-Hellman prime.																
ssl-hpkip *	Enable/disable including HPKP header in response.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HPKP header to each HTTP response.</td></tr><tr><td>enable</td><td>Add a HPKP header to each a HTTP response.</td></tr><tr><td>report-only</td><td>Add a HPKP Report-Only header to each HTTP response.</td></tr></table>	Option	Description	disable	Do not add a HPKP header to each HTTP response.	enable	Add a HPKP header to each a HTTP response.	report-only	Add a HPKP Report-Only header to each HTTP response.								
	Option	Description															
	disable	Do not add a HPKP header to each HTTP response.															
	enable	Add a HPKP header to each a HTTP response.															
report-only	Add a HPKP Report-Only header to each HTTP response.																
ssl-hpkip-age *	Number of seconds the client should honour the HPKP setting.	integer	Minimum value: 60 Maximum value: 157680000														
ssl-hpkip-backup *	Certificate to generate backup HPKP pin from.	string	Maximum length: 79														
ssl-hpkip-include-subdomains *	Indicate that HPKP header applies to all subdomains.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>HPKP header does not apply to subdomains.</td></tr><tr><td>enable</td><td>HPKP header applies to subdomains.</td></tr></table>	Option	Description	disable	HPKP header does not apply to subdomains.	enable	HPKP header applies to subdomains.										
	Option	Description															
	disable	HPKP header does not apply to subdomains.															
enable	HPKP header applies to subdomains.																
ssl-hpkip-primary *	Certificate to generate primary HPKP pin from.	string	Maximum length: 79														
ssl-hpkip-report-uri *	URL to report HPKP violations to.	var-string	Maximum length: 255														
ssl-hsts *	Enable/disable including HSTS header in response.	option	-														

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add a HSTS header to each a HTTP response.</td></tr><tr><td><i>enable</i></td><td>Add a HSTS header to each HTTP response.</td></tr></table>	Option	Description	<i>disable</i>	Do not add a HSTS header to each a HTTP response.	<i>enable</i>	Add a HSTS header to each HTTP response.								
Option	Description														
<i>disable</i>	Do not add a HSTS header to each a HTTP response.														
<i>enable</i>	Add a HSTS header to each HTTP response.														
ssl-hsts-age *	Number of seconds the client should honour the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000												
ssl-hsts-include-subdomains *	Indicate that HSTS header applies to all subdomains.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>HSTS header does not apply to subdomains.</td></tr><tr><td><i>enable</i></td><td>HSTS header applies to subdomains.</td></tr></table>	Option	Description	<i>disable</i>	HSTS header does not apply to subdomains.	<i>enable</i>	HSTS header applies to subdomains.								
Option	Description														
<i>disable</i>	HSTS header does not apply to subdomains.														
<i>enable</i>	HSTS header applies to subdomains.														
ssl-http-location-conversion *	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP location conversion.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP location conversion.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP location conversion.	<i>disable</i>	Disable HTTP location conversion.								
Option	Description														
<i>enable</i>	Enable HTTP location conversion.														
<i>disable</i>	Disable HTTP location conversion.														
ssl-http-match-host *	Enable/disable HTTP host matching for location conversion.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match HTTP host in response header.</td></tr><tr><td><i>disable</i></td><td>Do not match HTTP host.</td></tr></table>	Option	Description	<i>enable</i>	Match HTTP host in response header.	<i>disable</i>	Do not match HTTP host.								
Option	Description														
<i>enable</i>	Match HTTP host in response header.														
<i>disable</i>	Do not match HTTP host.														
ssl-max-version *	Highest SSL/TLS version acceptable from a client.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.		
Option	Description														
<i>ssl-3.0</i>	SSL 3.0.														
<i>tls-1.0</i>	TLS 1.0.														
<i>tls-1.1</i>	TLS 1.1.														
<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.														

Parameter	Description	Type	Size												
ssl-min-version *	Lowest SSL/TLS version acceptable from a client.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.		
Option	Description														
ssl-3.0	SSL 3.0.														
tls-1.0	TLS 1.0.														
tls-1.1	TLS 1.1.														
tls-1.2	TLS 1.2.														
tls-1.3	TLS 1.3.														
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	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>half</td><td>Client to FortiGate SSL.</td></tr><tr><td>full</td><td>Client to FortiGate and FortiGate to Server SSL.</td></tr></table>	Option	Description	half	Client to FortiGate SSL.	full	Client to FortiGate and FortiGate to Server SSL.								
Option	Description														
half	Client to FortiGate SSL.														
full	Client to FortiGate and FortiGate to Server SSL.														
ssl-pfs *	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>require</td><td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td></tr><tr><td>deny</td><td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td></tr><tr><td>allow</td><td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td></tr></table>	Option	Description	require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.						
Option	Description														
require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.														
deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.														
allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.														
ssl-send-empty-frags *	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Send empty fragments.</td></tr><tr><td>disable</td><td>Do not send empty fragments.</td></tr></table>	Option	Description	enable	Send empty fragments.	disable	Do not send empty fragments.								
Option	Description														
enable	Send empty fragments.														
disable	Do not send empty fragments.														
ssl-server-algorithm *	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-												

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td><i>custom</i></td><td>Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td><i>client</i></td><td>Use the same encryption algorithms for both client and server sessions.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	<i>custom</i>	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for both client and server sessions.				
	Option	Description															
	<i>high</i>	High encryption. Allow only AES and ChaCha.															
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.															
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.															
	<i>custom</i>	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.															
<i>client</i>	Use the same encryption algorithms for both client and server sessions.																
ssl-server-max-version *	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.		
	Option	Description															
	<i>ssl-3.0</i>	SSL 3.0.															
	<i>tls-1.0</i>	TLS 1.0.															
	<i>tls-1.1</i>	TLS 1.1.															
	<i>tls-1.2</i>	TLS 1.2.															
	<i>tls-1.3</i>	TLS 1.3.															
<i>client</i>	Use same value as client configuration.																
ssl-server-min-version *	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.		
	Option	Description															
	<i>ssl-3.0</i>	SSL 3.0.															
	<i>tls-1.0</i>	TLS 1.0.															
	<i>tls-1.1</i>	TLS 1.1.															
	<i>tls-1.2</i>	TLS 1.2.															
	<i>tls-1.3</i>	TLS 1.3.															
<i>client</i>	Use same value as client configuration.																
ssl-server-session-state-max *	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000														

Parameter	Description	Type	Size
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-type *	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-

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

type	Configure a static NAT, load balance, server load balance, DNS translation, or FQDN VIP.	option	-

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

uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-

Option	Description
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.
<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.

websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-

Option	Description
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.

* This parameter may not exist in some models.

config realservers

Parameter	Description	Type	Size								
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr><tr><td><i>vip</i></td><td>Use health check defined in VIP.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.		
	Option	Description									
	<i>disable</i>	Disable per server health check.									
	<i>enable</i>	Enable per server health check.									
<i>vip</i>	Use health check defined in VIP.										
holddown-interval	Time in seconds that the system waits before re-activating a previously down active server in the active-standby mode. This is to prevent any flapping issues.	integer	Minimum value: 30 Maximum value: 65535								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63								
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295								
ip	IP address of the real server.	ipv4-address-any	Not Specified								
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								
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	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>active</i>	Server status active.	
	<i>standby</i>	Server status standby.	
	<i>disable</i>	Server status disable.	
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255

config ssl-cipher-suites

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295
versions	SSL/TLS versions that the cipher suite can be used with.	option	-

Option	Description
<i>ssl-3.0</i>	SSL 3.0.
<i>tls-1.0</i>	TLS 1.0.

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

config ssl-server-cipher-suites

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

Parameter	Description	Type	Size

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

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295

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

Option	Description
<i>ssl-3.0</i>	SSL 3.0.
<i>tls-1.0</i>	TLS 1.0.
<i>tls-1.1</i>	TLS 1.1.
<i>tls-1.2</i>	TLS 1.2.
<i>tls-1.3</i>	TLS 1.3.

config firewall vip46

Configure IPv4 to IPv6 virtual IPs.

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

config firewall vip46

Parameter	Description	Type	Size						
arp-reply	Enable ARP reply.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable ARP reply.</td></tr><tr><td><i>enable</i></td><td>Enable ARP reply.</td></tr></table>			Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.
	Option	Description							
	<i>disable</i>	Disable ARP reply.							
<i>enable</i>	Enable ARP reply.								

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
extip	Start-external-IP [-end-external-IP].	user	Not Specified
extport	External service port.	user	Not Specified
id	Custom defined id.	integer	Minimum value: 0 Maximum value: 65535
ldb-method	Load balance method.	option	-
	Option	Description	
	<i>static</i>	Distribute sessions based on source IP.	
	<i>round-robin</i>	Distribute sessions based round robin order.	
	<i>weighted</i>	Distribute sessions based on weight.	
	<i>least-session</i>	Distribute sessions to the server with the lowest session count.	
	<i>least-rtt</i>	Distribute sessions to the server with the lowest Round-Trip-Time	
	<i>first-alive</i>	Distribute sessions to the first server that is alive.	
mappedip	Start-mapped-IP [-end mapped-IP].	user	Not Specified
mappedport	Mapped service port.	user	Not Specified
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79
name	VIP46 name.	string	Maximum length: 79
portforward	Enable port forwarding.	option	-
	Option	Description	
	<i>disable</i>	Disable port forwarding.	
	<i>enable</i>	Enable port forwarding.	
protocol	Mapped port protocol.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr></table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.						
	Option	Description											
	<i>tcp</i>	TCP.											
<i>udp</i>	UDP.												
server-type	Server type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>tcp</i></td><td>TCP</td></tr><tr><td><i>udp</i></td><td>UDP</td></tr><tr><td><i>ip</i></td><td>IP</td></tr></table>	Option	Description	<i>http</i>	HTTP	<i>tcp</i>	TCP	<i>udp</i>	UDP	<i>ip</i>	IP		
	Option	Description											
	<i>http</i>	HTTP											
	<i>tcp</i>	TCP											
	<i>udp</i>	UDP											
<i>ip</i>	IP												
src-filter <range>	Source IP filter (x.x.x.x/x). Src-filter range.	string	Maximum length: 79										
srcintf-filter <interface-name>	Interfaces to which the VIP46 applies. Separate the names with spaces. Interface name.	string	Maximum length: 79										
type	VIP type: static NAT or server load balance.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static-nat</i></td><td>Static NAT.</td></tr><tr><td><i>server-load-balance</i></td><td>Server load balance.</td></tr></table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.						
	Option	Description											
	<i>static-nat</i>	Static NAT.											
<i>server-load-balance</i>	Server load balance.												
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified										

config realservers

Parameter	Description	Type	Size								
client-ip	Restrict server to a client IP in this range.	user	Not Specified								
healthcheck	Per server health check.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr><tr><td><i>vip</i></td><td>Use health check defined in VIP.</td></tr></table>			Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.
Option	Description										
<i>disable</i>	Disable per server health check.										
<i>enable</i>	Enable per server health check.										
<i>vip</i>	Use health check defined in VIP.										

Parameter	Description	Type	Size
holddown-interval	Hold down interval.	integer	Minimum value: 30 Maximum value: 65535
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	Mapped server IPv6.	ipv6-address	Not Specified
max-connections	Maximum number of connections allowed to server.	integer	Minimum value: 0 Maximum value: 2147483647
monitor	Health monitors.	string	Maximum length: 79
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

config firewall vip6

Configure virtual IP for IPv6.

```
config firewall vip6
    Description: Configure virtual IP for IPv6.
    edit <name>
        set arp-reply [disable|enable]
        set color {integer}
        set comment {var-string}
```

```

set extip {user}
set extport {user}
set http-cookie-age {integer}
set http-cookie-domain {string}
set http-cookie-domain-from-host [disable|enable]
set http-cookie-generation {integer}
set http-cookie-path {string}
set http-cookie-share [disable|same-ip]
set http-ip-header [enable|disable]
set http-ip-header-name {string}
set http-multiplex [enable|disable]
set http-redirect [enable|disable]
set https-cookie-secure [disable|enable]
set id {integer}
set ldb-method [static|round-robin|...]
set mappedip {user}
set mappedport {user}
set max-embryonic-connections {integer}
set monitor <name1>, <name2>, ...
set outlook-web-access [disable|enable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set protocol [tcp|udp|...]
config realservers
    Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
    edit <id>
        set client-ip {user}
        set healthcheck [disable|enable|...]
        set holddown-interval {integer}
        set http-host {string}
        set ip {ipv6-address}
        set max-connections {integer}
        set monitor {string}
        set port {integer}
        set status [active|standby|...]
        set weight {integer}
    next
end
set server-type [http|https|...]
set src-filter <range1>, <range2>, ...
set ssl-algorithm [high|medium|...]
set ssl-certificate {string}
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-client-fallback [disable|enable]
set ssl-client-rekey-count {integer}
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-max {integer}
set ssl-client-session-state-timeout {integer}

```

```

set ssl-client-session-state-type [disable|time|...]
set ssl-dh-bits [768|1024|...]
set ssl-hpkip [disable|enable|...]
set ssl-hpkip-age {integer}
set ssl-hpkip-backup {string}
set ssl-hpkip-include-subdomains [disable|enable]
set ssl-hpkip-primary {string}
set ssl-hpkip-report-uri {var-string}
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-mode [half|full]
set ssl-pfs [require|deny|...]
set ssl-send-empty-frags [enable|disable]
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-session-state-max {integer}
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-type [disable|time|...]
set type [static-nat|server-load-balance]
set uuid {uuid}
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
next
end

```

config firewall vip6

Parameter	Description	Type	Size
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-
Option	Description		
<i>disable</i>	Disable ARP reply.		
<i>enable</i>	Enable ARP reply.		

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified
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-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-

Option	Description
<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.

http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35
http-cookie-share	Control sharing of cookies across virtual servers. same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-

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

Parameter	Description	Type	Size						
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding HTTP header.</td></tr><tr><td><i>disable</i></td><td>Disable adding HTTP header.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding HTTP header.	<i>disable</i>	Disable adding HTTP header.		
Option	Description								
<i>enable</i>	Enable adding HTTP header.								
<i>disable</i>	Disable adding HTTP header.								
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35						
http-multiplex	Enable/disable HTTP multiplexing.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP session multiplexing.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP session multiplexing.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP session multiplexing.	<i>disable</i>	Disable HTTP session multiplexing.		
Option	Description								
<i>enable</i>	Enable HTTP session multiplexing.								
<i>disable</i>	Disable HTTP session multiplexing.								
http-redirect	Enable/disable redirection of HTTP to HTTPS	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirection of HTTP to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirection of HTTP to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.		
Option	Description								
<i>enable</i>	Enable redirection of HTTP to HTTPS.								
<i>disable</i>	Disable redirection of HTTP to HTTPS.								
https-cookie-secure *	Enable/disable verification that inserted HTTPS cookies are secure.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
Option	Description								
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.								
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.								
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535						
ldb-method	Method used to distribute sessions to real servers.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute sessions based on source IP.</td></tr></table>	Option	Description	<i>static</i>	Distribute sessions based on source IP.				
Option	Description								
<i>static</i>	Distribute sessions based on source IP.								

Parameter	Description	Type	Size

Option	Description
<i>round-robin</i>	Distribute sessions based round robin order.
<i>weighted</i>	Distribute sessions based on weight.
<i>least-session</i>	Sends new sessions to the server with the lowest session count.
<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.
<i>first-alive</i>	Distribute sessions to the first server that is alive.
<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.

mappedip	Mapped IP address range in the format startIP-endIP.	user	Not Specified
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79
name	Virtual ip6 name.	string	Maximum length: 79
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-

Option	Description
<i>disable</i>	Disable Outlook Web Access support.
<i>enable</i>	Enable Outlook Web Access support.

persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-

Option	Description
<i>none</i>	None.
<i>http-cookie</i>	HTTP cookie.
<i>ssl-session-id</i>	SSL session ID.

Parameter	Description	Type	Size
portforward	Enable port forwarding.	option	-
	Option	Description	
	<i>disable</i>	Disable port forward.	
	<i>enable</i>	Enable/disable port forwarding.	
protocol	Protocol to use when forwarding packets.	option	-
	Option	Description	
	<i>tcp</i>	TCP.	
	<i>udp</i>	UDP.	
	<i>sctp</i>	SCTP.	
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-
	Option	Description	
	<i>http</i>	HTTP	
	<i>https</i>	HTTPS	
	<i>imaps</i>	IMAPS	
	<i>pop3s</i>	POP3S	
	<i>smtps</i>	SMTPS	
	<i>ssl</i>	SSL	
	<i>tcp</i>	TCP	
	<i>udp</i>	UDP	
<i>ip</i>	IP		
src-filter <range>	Source IP6 filter (x:x:x:x:x:x/x). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79
ssl-algorithm *	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-
	Option	Description	
	<i>high</i>	Use AES or 3DES.	
	<i>medium</i>	Use AES, 3DES, or RC4.	

Parameter	Description	Type	Size
	Option	Description	
	<i>low</i>	Use AES, 3DES, RC4, or DES.	
	<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.	
ssl-certificate *	The name of the SSL certificate to use for SSL acceleration.	string	Maximum length: 35
ssl-client-fallback *	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-
	Option	Description	
	<i>disable</i>	Disable.	
	<i>enable</i>	Enable.	
ssl-client-rekey-count *	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576
ssl-client-renegotiation *	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-
	Option	Description	
	<i>allow</i>	Allow a SSL client to renegotiate.	
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	
	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.	
ssl-client-session-state-max *	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000
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-type *	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-

Parameter	Description	Type	Size

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

ssl-dh-bits *	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-

Option	Description
768	768-bit Diffie-Hellman prime.
1024	1024-bit Diffie-Hellman prime.
1536	1536-bit Diffie-Hellman prime.
2048	2048-bit Diffie-Hellman prime.
3072	3072-bit Diffie-Hellman prime.
4096	4096-bit Diffie-Hellman prime.

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

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

ssl-hpkip-age *	Number of minutes the web browser should keep HPKP.	integer	Minimum value: 60 Maximum value: 157680000

ssl-hpkip-backup *	Certificate to generate backup HPKP pin from.	string	Maximum length: 79

ssl-hpkip-include-subdomains *	Indicate that HPKP header applies to all subdomains.	option	-

Option	Description
<i>disable</i>	HPKP header does not apply to subdomains.
<i>enable</i>	HPKP header applies to subdomains.

Parameter	Description	Type	Size
ssl-hpkp-primary *	Certificate to generate primary HPKP pin from.	string	Maximum length: 79
ssl-hpkp-report-uri *	URL to report HPKP violations to.	var-string	Maximum length: 255
ssl-hsts *	Enable/disable including HSTS header in response.	option	-

Option	Description

<i>disable</i>	Do not add a HSTS header to each a HTTP response.

<i>enable</i>	Add a HSTS header to each HTTP response.

ssl-hsts-age *	Number of seconds the client should honour the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000

ssl-hsts-include-subdomains *	Indicate that HSTS header applies to all subdomains.	option	-

Option	Description

<i>disable</i>	HSTS header does not apply to subdomains.

<i>enable</i>	HSTS header applies to subdomains.

ssl-http-location-conversion *	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-

Option	Description

<i>enable</i>	Enable HTTP location conversion.

<i>disable</i>	Disable HTTP location conversion.

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

Option	Description

<i>enable</i>	Match HTTP host in response header.

<i>disable</i>	Do not match HTTP host.

ssl-max-version *	Highest SSL/TLS version acceptable from a client.	option	-

Parameter	Description	Type	Size

Option	Description
<i>ssl-3.0</i>	SSL 3.0.
<i>tls-1.0</i>	TLS 1.0.
<i>tls-1.1</i>	TLS 1.1.
<i>tls-1.2</i>	TLS 1.2.
<i>tls-1.3</i>	TLS 1.3.

ssl-min-version *	Lowest SSL/TLS version acceptable from a client.	option	-

Option	Description
<i>ssl-3.0</i>	SSL 3.0.
<i>tls-1.0</i>	TLS 1.0.
<i>tls-1.1</i>	TLS 1.1.
<i>tls-1.2</i>	TLS 1.2.
<i>tls-1.3</i>	TLS 1.3.

ssl-mode *	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-

Option	Description
<i>half</i>	Client to FortiGate SSL.
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.

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

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

ssl-send-empty-frags *	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send empty fragments.</td></tr><tr><td><i>disable</i></td><td>Do not send empty fragments.</td></tr></table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.										
Option	Description																
<i>enable</i>	Send empty fragments.																
<i>disable</i>	Do not send empty fragments.																
ssl-server-algorithm *	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>Use AES or 3DES.</td></tr><tr><td><i>medium</i></td><td>Use AES, 3DES, or RC4.</td></tr><tr><td><i>low</i></td><td>Use AES, 3DES, RC4, or DES.</td></tr><tr><td><i>custom</i></td><td>Use config ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td><i>client</i></td><td>Use the same encryption algorithms for client and server sessions.</td></tr></table>	Option	Description	<i>high</i>	Use AES or 3DES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for client and server sessions.				
Option	Description																
<i>high</i>	Use AES or 3DES.																
<i>medium</i>	Use AES, 3DES, or RC4.																
<i>low</i>	Use AES, 3DES, RC4, or DES.																
<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.																
<i>client</i>	Use the same encryption algorithms for client and server sessions.																
ssl-server-max-version *	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.		
Option	Description																
<i>ssl-3.0</i>	SSL 3.0.																
<i>tls-1.0</i>	TLS 1.0.																
<i>tls-1.1</i>	TLS 1.1.																
<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																
<i>client</i>	Use same value as client configuration.																
ssl-server-min-version *	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.		
Option	Description																
<i>ssl-3.0</i>	SSL 3.0.																
<i>tls-1.0</i>	TLS 1.0.																
<i>tls-1.1</i>	TLS 1.1.																
<i>tls-1.2</i>	TLS 1.2.																
<i>tls-1.3</i>	TLS 1.3.																
<i>client</i>	Use same value as client configuration.																

Parameter	Description	Type	Size
ssl-server-session-state-max *	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000
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-type *	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-

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

type	Configure a static NAT or server load balance VIP.	option	-

Option	Description
<i>static-nat</i>	Static NAT.
<i>server-load-balance</i>	Server load balance.

uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-

Option	Description
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.
<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.

websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-

Option	Description
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.

* This parameter may not exist in some models.

config realservers

Parameter	Description	Type	Size								
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr><tr><td><i>vip</i></td><td>Use health check defined in VIP.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.		
Option	Description										
<i>disable</i>	Disable per server health check.										
<i>enable</i>	Enable per server health check.										
<i>vip</i>	Use health check defined in VIP.										
holddown-interval	Time in seconds that the system waits before re-activating a previously down active server in the active-standby mode. This is to prevent any flapping issues.	integer	Minimum value: 30 Maximum value: 65535								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63								
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295								
ip	IPv6 address of the real server.	ipv6-address	Not Specified								
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								
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	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>active</i>	Server status active.	
	<i>standby</i>	Server status standby.	
	<i>disable</i>	Server status disable.	
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255

config ssl-cipher-suites

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.		
	Option	Description																					
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																					
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																					
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																					
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																					
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																					
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																					
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																					
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																					
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																						
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295																				
versions	SSL/TLS versions that the cipher suite can be used with.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.																
	Option	Description																					
	<i>ssl-3.0</i>	SSL 3.0.																					
<i>tls-1.0</i>	TLS 1.0.																						

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

config ssl-server-cipher-suites

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

Parameter	Description	Type	Size

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

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

Parameter	Description	Type	Size

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

Parameter	Description	Type	Size

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

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

Parameter	Description	Type	Size

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

priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295

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

Option	Description
<i>ssl-3.0</i>	SSL 3.0.
<i>tls-1.0</i>	TLS 1.0.
<i>tls-1.1</i>	TLS 1.1.
<i>tls-1.2</i>	TLS 1.2.
<i>tls-1.3</i>	TLS 1.3.

config firewall vip64

Configure IPv6 to IPv4 virtual IPs.

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

config firewall vip64

Parameter	Description	Type	Size
arp-reply	Enable ARP reply.	option	-
	Option	Description	
	<i>disable</i>	Disable arp reply.	
	<i>enable</i>	Enable arp reply.	

Parameter	Description	Type	Size
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
extip	Start-external-IP [-end-external-IP].	user	Not Specified
extport	External service port.	user	Not Specified
id	Custom defined id.	integer	Minimum value: 0 Maximum value: 65535
ldb-method	Load balance method.	option	-

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

mappedip	Start-mapped-IP [-end-mapped-IP].	user	Not Specified
mappedport	Mapped service port.	user	Not Specified
monitor <name>	Health monitors. Health monitor name.	string	Maximum length: 79
name	VIP64 name.	string	Maximum length: 79
portforward	Enable port forwarding.	option	-

Option	Description
<i>disable</i>	Disable port forwarding.
<i>enable</i>	Enable port forwarding.

Parameter	Description	Type	Size										
protocol	Mapped port protocol.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp</td><td>TCP.</td></tr><tr><td>udp</td><td>UDP.</td></tr></table>	Option	Description	tcp	TCP.	udp	UDP.						
	Option	Description											
	tcp	TCP.											
udp	UDP.												
server-type	Server type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP</td></tr><tr><td>tcp</td><td>TCP</td></tr><tr><td>udp</td><td>UDP</td></tr><tr><td>ip</td><td>IP</td></tr></table>	Option	Description	http	HTTP	tcp	TCP	udp	UDP	ip	IP		
	Option	Description											
	http	HTTP											
	tcp	TCP											
	udp	UDP											
ip	IP												
src-filter <range>	Source IP6 filter (x:x:x:x:x:x/x). Src-filter range.	string	Maximum length: 79										
type	VIP type: static NAT or server load balance.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static-nat</td><td>Static NAT.</td></tr><tr><td>server-load-balance</td><td>Server load balance.</td></tr></table>	Option	Description	static-nat	Static NAT.	server-load-balance	Server load balance.						
	Option	Description											
	static-nat	Static NAT.											
server-load-balance	Server load balance.												
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified										

config realservers

Parameter	Description	Type	Size
client-ip	Restrict server to a client IP in this range.	user	Not Specified
healthcheck	Per server health check.	option	-
	OptionDescription		
	disable	Disable per server health check.	
	enable	Enable per server health check.	
	vip	Use health check defined in VIP.	

Parameter	Description	Type	Size
holddown-interval	Hold down interval.	integer	Minimum value: 30 Maximum value: 65535
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	Mapped server IP.	ipv4-address-any	Not Specified
max-connections	Maximum number of connections allowed to server.	integer	Minimum value: 0 Maximum value: 2147483647
monitor	Health monitors.	string	Maximum length: 79
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

config firewall vipgrp

Configure IPv4 virtual IP groups.

```
config firewall vipgrp
    Description: Configure IPv4 virtual IP groups.
    edit <name>
        set color {integer}
```



```

        set comments {var-string}
        set interface {string}
        set member <name1>, <name2>, ...
        set uuid {uuid}
    next
end

```

config firewall vipgrp

Parameter	Description	Type	Size
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32
comments	Comment.	var-string	Maximum length: 255
interface	interface	string	Maximum length: 35
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79
name	VIP group name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

config firewall vipgrp46

Configure IPv4 to IPv6 virtual IP groups.

```

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

```

config firewall vipgrp46

Parameter	Description	Type	Size
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32
comments	Comment.	var-string	Maximum length: 255
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP46 name.	string	Maximum length: 79
name	VIP46 group name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

config firewall vipgrp6

Configure IPv6 virtual IP groups.

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

config firewall vipgrp6

Parameter	Description	Type	Size
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32
comments	Comment.	var-string	Maximum length: 255
member <name>	Member VIP objects of the group (Separate multiple objects with a space).	string	Maximum length: 79

Parameter	Description	Type	Size
	IPv6 VIP name.		
name	IPv6 VIP group name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

config firewall vipgrp64

Configure IPv6 to IPv4 virtual IP groups.

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

config firewall vipgrp64

Parameter	Description	Type	Size
color	Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).	integer	Minimum value: 0 Maximum value: 32
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
name	VIP64 group name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified

config firewall wildcard-fqdn custom

Config global/VDOM Wildcard FQDN address.

```

config firewall wildcard-fqdn custom
    Description: Config global/VDOM Wildcard FQDN address.
    edit <name>
        set color {integer}
        set comment {var-string}
        set uuid {uuid}
        set visibility [enable|disable]
        set wildcard-fqdn {string}
    next
end

```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32
comment	Comment.	var-string	Maximum length: 255
name	Address name.	string	Maximum length: 79
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified
visibility	Enable/disable address visibility.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255

config firewall wildcard-fqdn group

Config global Wildcard FQDN address groups.

```

config firewall wildcard-fqdn group
    Description: Config global Wildcard FQDN address groups.
    edit <name>
        set color {integer}
        set comment {var-string}
        set member <name1>, <name2>, ...
        set uuid {uuid}
        set visibility [enable|disable]
    end
end

```

```
next
end
```

config firewall wildcard-fqdn group

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

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 406](#)

config ftp-proxy explicit

Configure explicit FTP proxy settings.

```
config ftp-proxy explicit
    Description: Configure explicit FTP proxy settings.
    set incoming-ip {ipv4-address-any}
    set incoming-port {user}
    set outgoing-ip {ipv4-address-any}
    set sec-default-action [accept|deny]
    set ssl [enable|disable]
    set ssl-algorithm [high|medium|...]
    set ssl-cert {string}
    set ssl-dh-bits [768|1024|...]
    set status [enable|disable]
end
```

config ftp-proxy explicit

Parameter	Description	Type	Size
incoming-ip	Accept incoming FTP requests from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-
		Option	Description
		<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not
		<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.
ssl	Enable/disable the explicit FTPS proxy.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable the explicit FTPS proxy.	
	<i>disable</i>	Disable the explicit FTPS proxy.	
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-
	Option	Description	
	<i>high</i>	High encryption. Allow only AES and ChaCha	
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	
ssl-cert	Name of certificate for SSL connections to this server (default = "Fortinet_CA_SSL").	string	Maximum length: 35
ssl-dh-bits	Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).	option	-
	Option	Description	
	<i>768</i>	768-bit Diffie-Hellman prime.	
	<i>1024</i>	1024-bit Diffie-Hellman prime.	
	<i>1536</i>	1536-bit Diffie-Hellman prime.	
	<i>2048</i>	2048-bit Diffie-Hellman prime.	
status	Enable/disable the explicit FTP proxy.	option	-
	Option	Description	
	<i>enable</i>	Enable the explicit FTP proxy.	
	<i>disable</i>	Disable the explicit FTP proxy.	

icap

This section includes syntax for the following commands:

- [config icap profile on page 408](#)
- [config icap server on page 411](#)

config icap profile

Configure ICAP profiles.

```
config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    config icap-headers
      Description: Configure ICAP forwarded request headers.
      edit <id>
        set base64-encoding [disable|enable]
        set content {string}
        set name {string}
      next
    end
    set methods {option1}, {option2}, ...
    set preview [disable|enable]
    set preview-data-length {integer}
    set replacemsg-group {string}
    set request [disable|enable]
    set request-failure [error|bypass]
    set request-path {string}
    set request-server {string}
    set response [disable|enable]
    set response-failure [error|bypass]
    set response-path {string}
    set response-req-hdr [disable|enable]
    set response-server {string}
    set streaming-content-bypass [disable|enable]
  next
end
```

config icap profile

Parameter	Description	Type	Size
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.	
	<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.	
	<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.	
	<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.	
	<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.	
	<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.	
	<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.	
	<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.	
name	ICAP profile name.	string	Maximum length: 35
preview	Enable/disable preview of data to ICAP server.	option	-
	Option	Description	
	<i>disable</i>	Disable preview of data to ICAP server.	
	<i>enable</i>	Enable preview of data to ICAP server.	
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096
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	
	<i>disable</i>	Disable HTTP request passing to ICAP server.	
	<i>enable</i>	Enable HTTP request passing to ICAP server.	

Parameter	Description	Type	Size						
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error.</td></tr><tr><td><i>bypass</i></td><td>Bypass.</td></tr></table>	Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.		
Option	Description								
<i>error</i>	Error.								
<i>bypass</i>	Bypass.								
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127						
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 35						
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable HTTP response passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP response passing to ICAP server.</td></tr></table>	Option	Description	<i>disable</i>	Disable HTTP response passing to ICAP server.	<i>enable</i>	Enable HTTP response passing to ICAP server.		
Option	Description								
<i>disable</i>	Disable HTTP response passing to ICAP server.								
<i>enable</i>	Enable HTTP response passing to ICAP server.								
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error.</td></tr><tr><td><i>bypass</i></td><td>Bypass.</td></tr></table>	Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.		
Option	Description								
<i>error</i>	Error.								
<i>bypass</i>	Bypass.								
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127						
response-req-hdr	Enable/disable addition of req-hdr for ICAP response modification (respmod) processing.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add req-hdr for response modification (respmod) processing.</td></tr><tr><td><i>enable</i></td><td>Add req-hdr for response modification (respmod) processing.</td></tr></table>	Option	Description	<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.	<i>enable</i>	Add req-hdr for response modification (respmod) processing.		
Option	Description								
<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.								
<i>enable</i>	Add req-hdr for response modification (respmod) processing.								
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 35						
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable bypassing of ICAP server for streaming content.	
	<i>enable</i>	Enable bypassing of ICAP server for streaming content.	

config icap-headers

Parameter	Description	Type	Size
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-
	Option	Description	
	<i>disable</i>	Disable use of base64 encoding of HTTP content.	
	<i>enable</i>	Enable use of base64 encoding of HTTP content.	
content	HTTP header content.	string	Maximum length: 255
id	HTTP forwarded header ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	HTTP forwarded header name.	string	Maximum length: 79

config icap server

Configure ICAP servers.

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

config icap server

Parameter	Description	Type	Size
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified
ip-version	IP version.	option	-
	Option		Description
	4	IPv4 ICAP address.	
	6	IPv6 ICAP address.	
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified
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
name	Server name.	string	Maximum length: 35
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535

ips

This section includes syntax for the following commands:

- [config ips custom on page 413](#)
- [config ips decoder on page 415](#)
- [config ips global on page 415](#)
- [config ips rule-settings on page 422](#)
- [config ips rule on page 419](#)
- [config ips sensor on page 422](#)
- [config ips settings on page 431](#)
- [config ips view-map on page 432](#)

config ips custom

Configure IPS custom signature.

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

config ips custom

Parameter	Description	Type	Size
action	Default action (pass or block) for this signature.	option	-

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

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable status.	
tag	Signature tag.	string	Maximum length: 63

config ips decoder

Configure IPS decoder. Read-only.

```
config ips decoder
    Description: Configure IPS decoder. Read-only.
    edit <name>
        config parameter
            Description: IPS group parameters. Read-only.
            edit <name>
                set value {string}
            next
        end
    next
end
```

config ips decoder

Parameter	Description	Type	Size
name	Decoder name.	string	Maximum length: 63

config parameter

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

config ips global

Configure IPS global parameter.

```
config ips global
    Description: Configure IPS global parameter.
```

```

set anomaly-mode [periodical|continuous]
set cp-accel-mode [none|basic|...]
set database [regular|extended]
set deep-app-insp-db-limit {integer}
set deep-app-insp-timeout {integer}
set engine-count {integer}
set exclude-signatures [none|industrial]
set fail-open [enable|disable]
set intelligent-mode [enable|disable]
set ips-reserve-cpu [disable|enable]
set np-accel-mode [none|basic]
set packet-log-queue-depth {integer}
set session-limit-mode [accurate|heuristic]
set skype-client-public-ipaddr {var-string}
set socket-size {integer}
set sync-session-ttl [enable|disable]
config tls-active-probe
    Description: TLS active probe configuration.
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set vdom {string}
end
set traffic-submit [enable|disable]
end

```

config ips global

Parameter	Description	Type	Size								
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once an anomaly is detected. Overrides individual anomaly settings.</td></tr></table>			Option	Description	<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.	<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.		
Option	Description										
<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.										
<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.										
cp-accel-mode *	IPS Pattern matching acceleration/offloading to CPx processors.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>CPx acceleration/offloading disabled.</td></tr><tr><td><i>basic</i></td><td>Offload basic pattern matching to CPx processors.</td></tr><tr><td><i>advanced</i></td><td>Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.</td></tr></table>			Option	Description	<i>none</i>	CPx acceleration/offloading disabled.	<i>basic</i>	Offload basic pattern matching to CPx processors.	<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.
Option	Description										
<i>none</i>	CPx acceleration/offloading disabled.										
<i>basic</i>	Offload basic pattern matching to CPx processors.										
<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.										

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>IPS regular database package.</td></tr><tr><td><i>extended</i></td><td>IPS extended database package.</td></tr></table>	Option	Description	<i>regular</i>	IPS regular database package.	<i>extended</i>	IPS extended database package.		
Option	Description								
<i>regular</i>	IPS regular database package.								
<i>extended</i>	IPS extended database package.								
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database (1 - 2147483647, 0 = use recommended setting)	integer	Minimum value: 0 Maximum value: 2147483647						
deep-app-insp-timeout	Timeout for Deep application inspection (1 - 2147483647 sec., 0 = use recommended setting).	integer	Minimum value: 0 Maximum value: 2147483647						
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255						
exclude-signatures	Excluded signatures.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No signatures excluded.</td></tr><tr><td><i>industrial</i></td><td>Exclude industrial signatures.</td></tr></table>	Option	Description	<i>none</i>	No signatures excluded.	<i>industrial</i>	Exclude industrial signatures.		
Option	Description								
<i>none</i>	No signatures excluded.								
<i>industrial</i>	Exclude industrial signatures.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS fail open.</td></tr><tr><td><i>disable</i></td><td>Disable IPS fail open.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS fail open.	<i>disable</i>	Disable IPS fail open.		
Option	Description								
<i>enable</i>	Enable IPS fail open.								
<i>disable</i>	Disable IPS fail open.								
intelligent-mode	Enable/disable IPS adaptive scanning (intelligent mode). Intelligent mode optimizes the scanning method for the type of traffic.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intelligent scan mode.</td></tr><tr><td><i>disable</i></td><td>Disable intelligent scan mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable intelligent scan mode.	<i>disable</i>	Disable intelligent scan mode.		
Option	Description								
<i>enable</i>	Enable intelligent scan mode.								
<i>disable</i>	Disable intelligent scan mode.								
ips-reserve-cpu *	Enable/disable IPS daemon's use of CPUs other than CPU 0	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).</td></tr><tr><td><i>enable</i></td><td>Enable IPS daemon's use of CPUs other than CPU 0.</td></tr></table>	Option	Description	<i>disable</i>	Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).	<i>enable</i>	Enable IPS daemon's use of CPUs other than CPU 0.		
Option	Description								
<i>disable</i>	Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).								
<i>enable</i>	Enable IPS daemon's use of CPUs other than CPU 0.								
np-accel-mode *	Acceleration mode for IPS processing by NPx processors.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>NPx acceleration disabled.</td></tr><tr><td><i>basic</i></td><td>NPx acceleration enabled.</td></tr></table>	Option	Description	<i>none</i>	NPx acceleration disabled.	<i>basic</i>	NPx acceleration enabled.		
Option	Description								
<i>none</i>	NPx acceleration disabled.								
<i>basic</i>	NPx acceleration enabled.								
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096						
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accurate</i></td><td>Accurately count concurrent sessions, demands more resources.</td></tr><tr><td><i>heuristic</i></td><td>Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.</td></tr></table>	Option	Description	<i>accurate</i>	Accurately count concurrent sessions, demands more resources.	<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.		
Option	Description								
<i>accurate</i>	Accurately count concurrent sessions, demands more resources.								
<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.								
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						
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: 256 **						

Parameter	Description	Type	Size
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-
	Option	Description	
	<i>enable</i>	Enable use of kernel session TTL for IPS sessions.	
	<i>disable</i>	Disable use of kernel session TTL for IPS sessions.	
traffic-submit	Enable/disable submitting attack data found by this FortiGate to FortiGuard.	option	-
	Option	Description	
	<i>enable</i>	Enable traffic submit.	
	<i>disable</i>	Disable traffic submit.	

* This parameter may not exist in some models.

** Values may differ between models.

config tls-active-probe

Parameter	Description	Type	Size
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31

config ips rule

Configure IPS rules. Read-only.

```

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

```

config ips rule

Parameter	Description	Type	Size
action	Action. Read-only.	option	-
	Option	Description	
	<i>pass</i>	Pass or allow matching traffic.	
	<i>block</i>	Block or drop matching traffic.	
application	Vulnerable applications. Read-only.	user	Not Specified
date	Date. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
group	Group. Read-only.	string	Maximum length: 63
location	Vulnerable location. Read-only.	user	Not Specified
log	Enable/disable logging. Read-only.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable logging.	
	<i>enable</i>	Enable logging.	
log-packet	Enable/disable packet logging. Read-only.	option	-
	Option	Description	
	<i>disable</i>	Disable packet logging.	
	<i>enable</i>	Enable packet logging.	
name	Rule name.	string	Maximum length: 63
os	Vulnerable operation systems. Read-only.	user	Not Specified
rev	Revision. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
rule-id	Rule ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
service	Vulnerable service. Read-only.	user	Not Specified
severity	Severity. Read-only.	user	Not Specified
status	Enable/disable status. Read-only.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	

config metadata

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

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

config ips rule-settings

Configure IPS rule setting. Read-only.

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

config ips rule-settings

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

config ips sensor

Configure IPS sensor.

```
config ips sensor
    Description: Configure IPS sensor.
    edit <name>
        set block-malicious-url [disable|enable]
        set comment {var-string}
    config entries
        Description: IPS sensor filter.
        edit <id>
            set action [pass|block|...]
            set application {user}
```

```

        config exempt-ip
            Description: Traffic from selected source or destination IP addresses is
exempt from this signature.
            edit <id>
                set dst-ip {ipv4-classnet}
                set src-ip {ipv4-classnet}
            next
        end
        set location {user}
        set log [disable|enable]
        set log-attack-context [disable|enable]
        set log-packet [disable|enable]
        set os {user}
        set protocol {user}
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        set rule <id1>, <id2>, ...
        set severity {user}
        set status [disable|enable|...]
    next
end
set extended-log [enable|disable]
config filter
    Description: IPS sensor filter.
    edit <name>
        set action [pass|block|...]
        set application {user}
        set location {user}
        set log [disable|enable]
        set log-packet [disable|enable]
        set os {user}
        set protocol {user}
        set quarantine [none|attacker]
        set quarantine-expiry {integer}
        set quarantine-log [disable|enable]
        set severity {user}
        set status [disable|enable|...]
    next
end
config override
    Description: IPS override rule.
    edit <rule-id>
        set action [pass|block|...]
        config exempt-ip
            Description: Exempted IP.
            edit <id>
                set dst-ip {ipv4-classnet}
                set src-ip {ipv4-classnet}
            next
        end
        set log [disable|enable]

```

```

        set log-packet [disable|enable]
        set quarantine [none|attacker]
        set quarantine-expiry {integer}
        set quarantine-log [disable|enable]
        set status [disable|enable]
    next
end
set replacemsg-group {string}
set scan-botnet-connections [disable|block|...]
next
end

```

config ips sensor

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

* This parameter may not exist in some models.

config entries

Parameter	Description	Type	Size										
action	Action taken with traffic in which signatures are detected.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Pass or allow matching traffic.</td></tr><tr><td>block</td><td>Block or drop matching traffic.</td></tr><tr><td>reset</td><td>Reset sessions for matching traffic.</td></tr><tr><td>default</td><td>Pass or drop matching traffic, depending on the default action of the signature.</td></tr></table>	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.		
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.												
application	Applications to be protected. set application ? lists available applications. all includes all applications. other includes all unlisted applications.	user	Not Specified										
id	Rule ID in IPS database (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295										
location	Protect client or server traffic.	user	Not Specified										
log	Enable/disable logging of signatures included in filter.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of selected rules.</td></tr><tr><td>enable</td><td>Enable logging of selected rules.</td></tr></table>	Option	Description	disable	Disable logging of selected rules.	enable	Enable logging of selected rules.						
Option	Description												
disable	Disable logging of selected rules.												
enable	Enable logging of selected rules.												
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of detailed attack context.</td></tr><tr><td>enable</td><td>Enable logging of detailed attack context.</td></tr></table>	Option	Description	disable	Disable logging of detailed attack context.	enable	Enable logging of detailed attack context.						
Option	Description												
disable	Disable logging of detailed attack context.												
enable	Enable logging of detailed attack context.												
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	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable packet logging of selected rules.</td></tr><tr><td>enable</td><td>Enable packet logging of selected rules.</td></tr></table>	Option	Description	disable	Disable packet logging of selected rules.	enable	Enable packet logging of selected rules.						
Option	Description												
disable	Disable packet logging of selected rules.												
enable	Enable packet logging of selected rules.												

Parameter	Description	Type	Size
os	Operating systems to be protected. all includes all operating systems. other includes all unlisted operating systems.	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
quarantine	Quarantine method.	option	-

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

quarantine-expiry	Duration of quarantine. (Format ####d##h##m, minimum 1m, maximum 364d23h59m, default = 5m). Requires quarantine set to attacker.	user	Not Specified
quarantine-log	Enable/disable quarantine logging.	option	-

Option	Description
<i>disable</i>	Disable quarantine logging.
<i>enable</i>	Enable quarantine 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
<i>periodical</i>	Allow configured number of packets every rate-duration.
<i>continuous</i>	Block packets once the rate is reached.

rate-track	Track the packet protocol field.	option	-

Option	Description
<i>none</i>	none

Parameter	Description	Type	Size

Option	Description
<i>src-ip</i>	Source IP.
<i>dest-ip</i>	Destination IP.
<i>dhcp-client-mac</i>	DHCP client.
<i>dns-domain</i>	DNS domain.

rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified
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
<i>disable</i>	Disable status of selected rules.
<i>enable</i>	Enable status of selected rules.
<i>default</i>	Default.

config exempt-ip

Parameter	Description	Type	Size
dst-ip	Destination IP address and netmask.	ipv4-classnet	Not Specified
id	Exempt IP ID.	integer	Minimum value: 0 Maximum value: 4294967295
src-ip	Source IP address and netmask.	ipv4-classnet	Not Specified

config filter

Parameter	Description	Type	Size										
action	Action of selected rules.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr><tr><td><i>reset</i></td><td>Reset sessions for matching traffic.</td></tr><tr><td><i>default</i></td><td>Pass or drop matching traffic, depending on the default action of the signature.</td></tr></table>			Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.	<i>reset</i>	Reset sessions for matching traffic.	<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.
Option	Description												
<i>pass</i>	Pass or allow matching traffic.												
<i>block</i>	Block or drop matching traffic.												
<i>reset</i>	Reset sessions for matching traffic.												
<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.												
application	Vulnerable application filter.	user	Not Specified										
location	Vulnerability location filter.	user	Not Specified										
log	Enable/disable logging of selected rules.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable logging of selected rules.</td></tr></table>			Option	Description	<i>disable</i>	Disable logging of selected rules.	<i>enable</i>	Enable logging of selected rules.				
Option	Description												
<i>disable</i>	Disable logging of selected rules.												
<i>enable</i>	Enable logging of selected rules.												
log-packet	Enable/disable packet logging of selected rules.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging of selected rules.</td></tr></table>			Option	Description	<i>disable</i>	Disable packet logging of selected rules.	<i>enable</i>	Enable packet logging of selected rules.				
Option	Description												
<i>disable</i>	Disable packet logging of selected rules.												
<i>enable</i>	Enable packet logging of selected rules.												
name	Filter name.	string	Maximum length: 31										
os	Vulnerable OS filter.	user	Not Specified										
protocol	Vulnerable protocol filter.	user	Not Specified										
quarantine	Quarantine IP or interface.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>			Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.				
Option	Description												
<i>none</i>	Quarantine is disabled.												
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.												

Parameter	Description	Type	Size
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

<i>disable</i>	Disable logging of selected quarantine.

<i>enable</i>	Enable logging of selected quarantine.

severity	Vulnerability severity filter.	user	Not Specified
status	Selected rules status.	option	-

Option	Description

<i>disable</i>	Disable status of selected rules.

<i>enable</i>	Enable status of selected rules.

<i>default</i>	Default.

config override

Parameter	Description	Type	Size
action	Action of override rule.	option	-

Option	Description
<i>pass</i>	Pass or allow matching traffic.
<i>block</i>	Block or drop matching traffic.
<i>reset</i>	Reset sessions for matching traffic.

log	Enable/disable logging.	option	-

Option	Description
<i>disable</i>	Disable logging.
<i>enable</i>	Enable logging.

log-packet	Enable/disable packet logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable packet logging.	
	<i>enable</i>	Enable packet logging.	
quarantine	Quarantine IP or interface.	option	-
	Option	Description	
	<i>none</i>	Quarantine is disabled.	
	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.	
quarantine-expiry	Duration of quarantine in minute.	integer	Minimum value: 1 Maximum value: 2147483647
quarantine-log	Enable/disable logging of selected quarantine.	option	-
	Option	Description	
	<i>disable</i>	Disable logging of selected quarantine.	
	<i>enable</i>	Enable logging of selected quarantine.	
rule-id	Override rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
status	Enable/disable status of override rule.	option	-
	Option	Description	
	<i>disable</i>	Disable status of override rule.	
	<i>enable</i>	Enable status of override rule.	

config exempt-ip

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

Parameter	Description	Type	Size
id	Exempt IP ID.	integer	Minimum value: 0 Maximum value: 4294967295
src-ip	Source IP address and netmask.	ipv4-classnet	Not Specified

config ips settings

Configure IPS VDOM parameter.

```
config ips settings
    Description: Configure IPS VDOM parameter.
    set ips-packet-quota {integer}
    set packet-log-history {integer}
    set packet-log-memory {integer}
    set packet-log-post-attack {integer}
end
```

config ips settings

Parameter	Description	Type	Size
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
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected (1 - 255).	integer	Minimum value: 1 Maximum value: 255
packet-log-memory	Maximum memory can be used by packet log (64 - 8192 kB).	integer	Minimum value: 64 Maximum value: 8192
packet-log-post-attack	Number of packets to log after the IPS signature is detected (0 - 255).	integer	Minimum value: 0 Maximum value: 255

config ips view-map

configure ips view-map Read-only.

```
config ips view-map
  Description: configure ips view-map Read-only.
  edit <id>
    set id-policy-id {integer}
    set policy-id {integer}
    set vdom-id {integer}
    set which [firewall|firewall6|...]
  next
end
```

config ips view-map

Parameter	Description	Type	Size
id	View ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
id-policy-id	ID-based policy ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
policy-id	Policy ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
vdom-id	VDOM ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
which	Policy. Read-only.	option	-

Option	Description
<i>firewall</i>	Firewall policy.
<i>firewall6</i>	Firewall policy6.
<i>interface</i>	Interface policy.

Parameter	Description	Type	Size

Option	Description
<i>interface6</i>	Interface policy6.
<i>sniffer</i>	Sniffer policy.
<i>sniffer6</i>	Sniffer policy6.
<i>explicit</i>	explicit proxy policy.

log

This section includes syntax for the following commands:

- [config log custom-field on page 435](#)
- [config log disk filter on page 435](#)
- [config log disk setting on page 441](#)
- [config log eventfilter on page 446](#)
- [config log fortianalyzer-cloud filter on page 485](#)
- [config log fortianalyzer-cloud override-filter on page 487](#)
- [config log fortianalyzer-cloud override-setting on page 489](#)
- [config log fortianalyzer-cloud setting on page 490](#)
- [config log fortianalyzer2 filter on page 461](#)
- [config log fortianalyzer2 override-filter on page 463](#)
- [config log fortianalyzer2 override-setting on page 465](#)
- [config log fortianalyzer2 setting on page 469](#)
- [config log fortianalyzer3 filter on page 473](#)
- [config log fortianalyzer3 override-filter on page 475](#)
- [config log fortianalyzer3 override-setting on page 477](#)
- [config log fortianalyzer3 setting on page 481](#)
- [config log fortianalyzer filter on page 448](#)
- [config log fortianalyzer override-filter on page 450](#)
- [config log fortianalyzer override-setting on page 453](#)
- [config log fortianalyzer setting on page 457](#)
- [config log fortiguard filter on page 493](#)
- [config log fortiguard override-filter on page 495](#)
- [config log fortiguard override-setting on page 497](#)
- [config log fortiguard setting on page 499](#)
- [config log gui-display on page 501](#)
- [config log memory filter on page 502](#)
- [config log memory global-setting on page 507](#)
- [config log memory setting on page 508](#)
- [config log null-device filter on page 509](#)
- [config log null-device setting on page 511](#)
- [config log setting on page 511](#)
- [config log syslogd2 filter on page 528](#)
- [config log syslogd2 override-filter on page 530](#)
- [config log syslogd2 override-setting on page 532](#)
- [config log syslogd2 setting on page 536](#)
- [config log syslogd3 filter on page 540](#)

- [config log syslogd3 override-filter on page 542](#)
- [config log syslogd3 override-setting on page 544](#)
- [config log syslogd3 setting on page 548](#)
- [config log syslogd4 filter on page 552](#)
- [config log syslogd4 override-filter on page 554](#)
- [config log syslogd4 override-setting on page 556](#)
- [config log syslogd4 setting on page 560](#)
- [config log syslogd filter on page 516](#)
- [config log syslogd override-filter on page 518](#)
- [config log syslogd override-setting on page 520](#)
- [config log syslogd setting on page 524](#)
- [config log threat-weight on page 564](#)
- [config log webtrends filter on page 574](#)
- [config log webtrends setting on page 576](#)

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
id	field ID <string>.	string	Maximum length: 35
name	Field name (max: 15 characters).	string	Maximum length: 15
value	Field value (max: 15 characters).	string	Maximum length: 15

config log disk filter

Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type.

```

config log disk filter
    Description: Configure filters for local disk logging. Use these filters to determine
the log messages to record according to severity and type.
    set admin [enable|disable]
    set anomaly [enable|disable]
    set auth [enable|disable]
    set chassis-loadbalance-ha [enable|disable]
    set cpu-memory-usage [enable|disable]
    set dhcp [enable|disable]
    set dlp-archive [enable|disable]
    set event [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set ha [enable|disable]
    set ipsec [enable|disable]
    set ldb-monitor [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set pattern [enable|disable]
    set ppp [enable|disable]
    set radius [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set sslvpn-log-adm [enable|disable]
    set sslvpn-log-auth [enable|disable]
    set sslvpn-log-session [enable|disable]
    set system [enable|disable]
    set vip-ssl [enable|disable]
    set voip [enable|disable]
    set wan-opt [enable|disable]
    set wireless-activity [enable|disable]
end

```

config log disk filter

Parameter	Description	Type	Size						
admin	Enable/disable admin login/logout logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable admin login/logout logging.</td></tr><tr><td><i>disable</i></td><td>Disable admin login/logout logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable admin login/logout logging.	<i>disable</i>	Disable admin login/logout logging.		
Option	Description								
<i>enable</i>	Enable admin login/logout logging.								
<i>disable</i>	Disable admin login/logout logging.								
anomaly	Enable/disable anomaly logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.		
Option	Description								
<i>enable</i>	Enable anomaly logging.								
<i>disable</i>	Disable anomaly logging.								

Parameter	Description	Type	Size
auth	Enable/disable firewall authentication logging.	option	-
	Option	Description	
	<i>enable</i>	Enable firewall authentication logging.	
	<i>disable</i>	Disable firewall authentication logging.	
chassis-loadbalance-ha *	Enable/disable chassis load balancer state changes logging.	option	-
	Option	Description	
	<i>enable</i>	Enable chassis load balancer state changes logging.	
	<i>disable</i>	Disable chassis load balancer state changes logging.	
cpu-memory-usage	Enable/disable CPU & memory usage logging every 5 minutes.	option	-
	Option	Description	
	<i>enable</i>	Enable CPU & memory usage logging every 5 minutes.	
	<i>disable</i>	Disable CPU & memory usage logging every 5 minutes.	
dhcp	Enable/disable DHCP service messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DHCP service messages logging.	
	<i>disable</i>	Disable DHCP service messages logging.	
dlp-archive *	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	Disable DLP archive logging.	
event	Enable/disable event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
filter	Disk log filter.	string	Maximum length: 511

Parameter	Description	Type	Size						
filter-type	Include/exclude logs that match the filter.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.		
Option	Description								
<i>include</i>	Include logs that match the filter.								
<i>exclude</i>	Exclude logs that match the filter.								
forward-traffic	Enable/disable forward traffic logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.		
Option	Description								
<i>enable</i>	Enable forward traffic logging.								
<i>disable</i>	Disable forward traffic logging.								
gtp *	Enable/disable GTP messages logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.		
Option	Description								
<i>enable</i>	Enable GTP messages logging.								
<i>disable</i>	Disable GTP messages logging.								
ha	Enable/disable HA logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA logging.</td></tr><tr><td><i>disable</i></td><td>Disable HA logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable HA logging.	<i>disable</i>	Disable HA logging.		
Option	Description								
<i>enable</i>	Enable HA logging.								
<i>disable</i>	Disable HA logging.								
ipsec	Enable/disable IPsec negotiation messages logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec negotiation messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec negotiation messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec negotiation messages logging.	<i>disable</i>	Disable IPsec negotiation messages logging.		
Option	Description								
<i>enable</i>	Enable IPsec negotiation messages logging.								
<i>disable</i>	Disable IPsec negotiation messages logging.								
ldb-monitor	Enable/disable VIP real server health monitoring logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VIP real server health monitoring logging.</td></tr><tr><td><i>disable</i></td><td>Disable VIP real server health monitoring logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VIP real server health monitoring logging.	<i>disable</i>	Disable VIP real server health monitoring logging.		
Option	Description								
<i>enable</i>	Enable VIP real server health monitoring logging.								
<i>disable</i>	Disable VIP real server health monitoring logging.								
local-traffic	Enable/disable local in or out traffic logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.				
Option	Description								
<i>enable</i>	Enable local in or out traffic logging.								

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
pattern	Enable/disable pattern update logging.	option	-
	Option	Description	
	<i>enable</i>	Enable pattern update logging.	
	<i>disable</i>	Disable pattern update logging.	
ppp	Enable/disable L2TP/PPTP/PPPoE logging.	option	-
	Option	Description	
	<i>enable</i>	Enable L2TP/PPTP/PPPoE logging.	
	<i>disable</i>	Disable L2TP/PPTP/PPPoE logging.	
radius	Enable/disable RADIUS messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable RADIUS messages logging.	
	<i>disable</i>	Disable RADIUS messages logging.	
severity	Log to disk every message above and including this severity level.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	

Parameter	Description	Type	Size
	Option	Description	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sslvpn-log-adm	Enable/disable SSL administrator login logging.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL administrator logging.	
	<i>disable</i>	Disable SSL administrator logging.	
sslvpn-log-auth	Enable/disable SSL user authentication logging.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL user authentication logging.	
	<i>disable</i>	Disable SSL user authentication logging.	
sslvpn-log-session	Enable/disable SSL session logging.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL session logging.	
	<i>disable</i>	Disable SSL session logging.	
system	Enable/disable system activity logging.	option	-
	Option	Description	
	<i>enable</i>	Enable system activity logging.	
	<i>disable</i>	Disable system activity logging.	
vip-ssl *	Enable/disable VIP SSL logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VIP SSL logging.	
	<i>disable</i>	Disable VIP SSL logging.	

Parameter	Description	Type	Size						
voip	Enable/disable VoIP logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.		
Option	Description								
<i>enable</i>	Enable VoIP logging.								
<i>disable</i>	Disable VoIP logging.								
wan-opt	Enable/disable WAN optimization event logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN optimization event logging.</td></tr><tr><td><i>disable</i></td><td>Disable WAN optimization event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable WAN optimization event logging.	<i>disable</i>	Disable WAN optimization event logging.		
Option	Description								
<i>enable</i>	Enable WAN optimization event logging.								
<i>disable</i>	Disable WAN optimization event logging.								
wireless-activity	Enable/disable wireless activity event logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless activity event logging.</td></tr><tr><td><i>disable</i></td><td>Disable wireless activity event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable wireless activity event logging.	<i>disable</i>	Disable wireless activity event logging.		
Option	Description								
<i>enable</i>	Enable wireless activity event logging.								
<i>disable</i>	Disable wireless activity event logging.								

* This parameter may not exist in some models.

config log disk setting

Settings for local disk logging.

```
config log disk setting
    Description: Settings for local disk logging.
    set diskfull [overwrite|nolog]
    set dlp-archive-quota {integer}
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set ips-archive [enable|disable]
    set log-quota {integer}
    set max-log-file-size {integer}
    set max-policy-packet-capture-size {integer}
    set maximum-log-age {integer}
    set report-quota {integer}
    set roll-day {option1}, {option2}, ...
    set roll-schedule [daily|weekly]
    set roll-time {user}
    set source-ip {ipv4-address}
    set status [enable|disable]
    set upload [enable|disable]
    set upload-delete-files [enable|disable]
    set upload-destination {option}
```

```

set upload-ssl-conn [default|high|...]
set uploadaddr {string}
set uploadip {ipv4-address}
set uploadpass {password}
set uploadport {integer}
set uploadsched [disable|enable]
set uploadtime {user}
set uploadtype {option1}, {option2}, ...
set uploaduser {string}

```

end

config log disk setting

Parameter	Description	Type	Size						
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full (default = overwrite).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>overwrite</td><td>Overwrite the oldest logs when the log disk is full.</td></tr><tr><td>nolog</td><td>Stop logging when the log disk is full.</td></tr></table>			Option	Description	overwrite	Overwrite the oldest logs when the log disk is full.	nolog	Stop logging when the log disk is full.
Option	Description								
overwrite	Overwrite the oldest logs when the log disk is full.								
nolog	Stop logging when the log disk is full.								
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295						
full-final-warning-threshold	Log full final warning threshold as a percent (3 - 100, default = 95).	integer	Minimum value: 3 Maximum value: 100						
full-first-warning-threshold	Log full first warning threshold as a percent (1 - 98, default = 75).	integer	Minimum value: 1 Maximum value: 98						
full-second-warning-threshold	Log full second warning threshold as a percent (2 - 99, default = 90).	integer	Minimum value: 2 Maximum value: 99						
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS packet archiving.</td></tr></table>			Option	Description	enable	Enable IPS packet archiving.		
Option	Description								
enable	Enable IPS packet archiving.								

Parameter	Description	Type	Size

Option	Description
<i>disable</i>	Disable IPS packet archiving.

log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295
max-log-file-size	Maximum log file size before rolling (1 - 100 Mbytes).	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
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650
report-quota *	Report quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295
roll-day	Day of week on which to roll log file.	option	-

Option	Description
<i>sunday</i>	Sunday
<i>monday</i>	Monday
<i>tuesday</i>	Tuesday
<i>wednesday</i>	Wednesday
<i>thursday</i>	Thursday
<i>friday</i>	Friday
<i>saturday</i>	Saturday

roll-schedule	Frequency to check log file for rolling.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>daily</i>	Check the log file once a day.	
	<i>weekly</i>	Check the log file once a week.	
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified
status	Enable/disable local disk logging.	option	-
	Option	Description	
	<i>enable</i>	Log to local disk.	
	<i>disable</i>	Do not log to local disk.	
upload	Enable/disable uploading log files when they are rolled.	option	-
	Option	Description	
	<i>enable</i>	Enable uploading log files when they are rolled.	
	<i>disable</i>	Disable uploading log files when they are rolled.	
upload-delete-files	Delete log files after uploading (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Delete log files after uploading.	
	<i>disable</i>	Do not delete log files after uploading.	
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-
	Option	Description	
	<i>ftp-server</i>	Upload rolled log files to an FTP server.	
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-
	Option	Description	
	<i>default</i>	FTPS with high and medium encryption algorithms.	
	<i>high</i>	FTPS with high encryption algorithms.	
	<i>low</i>	FTPS with low encryption algorithms.	

Parameter	Description	Type	Size

Option	Description
<i>disable</i>	Disable FTPS communication.

uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified
uploadport	TCP port to use for communicating with the FTP server (default = 21).	integer	Minimum value: 0 Maximum value: 65535
uploadsched	Set the schedule for uploading log files to the FTP server (default = disable = upload when rolling).	option	-

Option	Description
<i>disable</i>	Upload when rolling.
<i>enable</i>	Scheduled upload.

uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-

Option	Description
<i>traffic</i>	Upload traffic log.
<i>event</i>	Upload event log.
<i>virus</i>	Upload anti-virus log.
<i>webfilter</i>	Upload web filter log.
<i>IPS</i>	Upload IPS log.
<i>emailfilter</i>	Upload spam filter log.
<i>dlp-archive</i>	Upload DLP archive.
<i>anomaly</i>	Upload anomaly log.
<i>voip</i>	Upload VoIP log.
<i>dlp</i>	Upload DLP log.

Parameter	Description	Type	Size
	Option	Description	
	<i>app-ctrl</i>	Upload application control log.	
	<i>waf</i>	Upload web application firewall log.	
	<i>dns</i>	Upload DNS log.	
	<i>ssh</i>	Upload SSH log.	
	<i>ssl</i>	Upload SSL log.	
	<i>cifs</i>	Upload CIFS log.	
	<i>file-filter</i>	Upload file-filter log.	
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35

* This parameter may not exist in some models.

config log eventfilter

Configure log event filters.

```
config log eventfilter
    Description: Configure log event filters.
    set connector [enable|disable]
    set endpoint [enable|disable]
    set event [enable|disable]
    set fortiextender [enable|disable]
    set ha [enable|disable]
    set router [enable|disable]
    set security-rating [enable|disable]
    set system [enable|disable]
    set user [enable|disable]
    set vpn [enable|disable]
    set wan-opt [enable|disable]
    set wireless-activity [enable|disable]
end
```

config log eventfilter

Parameter	Description	Type	Size
connector	Enable/disable SDN connector logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable SDN connector logging.	
	<i>disable</i>	Disable SDN connector logging.	
endpoint	Enable/disable endpoint event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable endpoint event logging.	
	<i>disable</i>	Disable endpoint event logging.	
event	Enable/disable event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable event logging.	
	<i>disable</i>	Disable event logging.	
fortiextender	Enable/disable FortiExtender logging.	option	-
	Option	Description	
	<i>enable</i>	Enable Forti-Extender logging.	
	<i>disable</i>	Disable Forti-Extender logging.	
ha	Enable/disable ha event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable ha event logging.	
	<i>disable</i>	Disable ha event logging.	
router	Enable/disable router event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable router event logging.	
	<i>disable</i>	Disable router event logging.	
security-rating	Enable/disable Security Rating result logging.	option	-
	Option	Description	
	<i>enable</i>	Enable Security Fabric audit result logging.	
	<i>disable</i>	Disable Security Fabric audit result logging.	
system	Enable/disable system event logging.	option	-

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

config log fortianalyzer filter

Filters for FortiAnalyzer.

```
config log fortianalyzer filter
  Description: Filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
```



```

set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
end

```

config log fortianalyzer filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	Disable DLP archive logging.	
filter	FortiAnalyzer log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VoIP logging.	
	<i>disable</i>	Disable VoIP logging.	

* This parameter may not exist in some models.

config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

```

config log fortianalyzer override-filter
    Description: Override filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end

```

config log fortianalyzer override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	Disable DLP archive logging.	
filter	FortiAnalyzer log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-

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

* This parameter may not exist in some models.

config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
    Description: Override FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
    set use-management-vdom [enable|disable]
end
```

config log fortianalyzer override-setting

Parameter	Description	Type	Size
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.	
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option	Description	
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option	Description	
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	
	<i>high</i>	Encrypt logs using high encryption algorithms.	
	<i>low</i>	Encrypt logs using all encryption algorithms.	
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option	Description	
	<i>sha256</i>	Use SHA256 as HMAC algorithm.	
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	

Parameter	Description	Type	Size
	Option	Description	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable IPS packet archive logging.	
	<i>disable</i>	Disable IPS packet archive logging.	
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
priority	Set log transmission priority.	option	-
	Option	Description	
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
server	The remote FortiAnalyzer.	string	Maximum length: 63
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63

Parameter	Description	Type	Size												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.		
Option	Description														
default	Follow system global setting.														
SSLv3	SSLv3.														
TLSv1	TLSv1.														
TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.														
status	Enable/disable logging to FortiAnalyzer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.								
Option	Description														
enable	Enable logging to FortiAnalyzer.														
disable	Disable logging to FortiAnalyzer.														
upload-day	Day of week (month) to upload logs.	user	Not Specified												
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.						
Option	Description														
daily	Upload log files to FortiAnalyzer once a day.														
weekly	Upload log files to FortiAnalyzer once a week.														
monthly	Upload log files to FortiAnalyzer once a month.														
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at most every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at most every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at most every 1 minute.	5-minute	Log directly to FortiAnalyzer at most every 5 minutes.				
Option	Description														
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.														
realtime	Log directly to FortiAnalyzer in real time.														
1-minute	Log directly to FortiAnalyzer at most every 1 minute.														
5-minute	Log directly to FortiAnalyzer at most every 5 minutes.														
upload-time	Time to upload logs (hh:mm).	user	Not Specified												
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-												

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

config log fortianalyzer setting

Global FortiAnalyzer settings.

```
config log fortianalyzer setting
    Description: Global FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end
```

config log fortianalyzer setting

Parameter	Description	Type	Size
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.	
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-
	Option	Description	
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option	Description	
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	
	<i>high</i>	Encrypt logs using high encryption algorithms.	
	<i>low</i>	Encrypt logs using all encryption algorithms.	
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option	Description	
	<i>sha256</i>	Use SHA256 as HMAC algorithm.	
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	

Parameter	Description	Type	Size
	Option	Description	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable IPS packet archive logging.	
	<i>disable</i>	Disable IPS packet archive logging.	
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
priority	Set log transmission priority.	option	-
	Option	Description	
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
server	The remote FortiAnalyzer.	string	Maximum length: 63

Parameter	Description	Type	Size
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	default	Follow system global setting.	
	SSLv3	SSLv3.	
	TLSv1	TLSv1.	
	TLSv1-1	TLSv1.1.	
	TLSv1-2	TLSv1.2.	
status	Enable/disable logging to FortiAnalyzer.	option	-
	Option	Description	
	enable	Enable logging to FortiAnalyzer.	
	disable	Disable logging to FortiAnalyzer.	
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option	Description	
	daily	Upload log files to FortiAnalyzer once a day.	
	weekly	Upload log files to FortiAnalyzer once a week.	
	monthly	Upload log files to FortiAnalyzer once a month.	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-
	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-time	Time to upload logs (hh:mm).	user	Not Specified

config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer2 filter
  Description: Filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
end
```

config log fortianalyzer2 filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	Disable DLP archive logging.	
filter	FortiAnalyzer 2 log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Log every message above and including this severity level.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

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

* This parameter may not exist in some models.

config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer2 override-filter
    Description: Override filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log fortianalyzer2 override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	Disable DLP archive logging.	
filter	FortiAnalyzer 2 log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Log every message above and including this severity level.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VoIP logging.	
	<i>disable</i>	Disable VoIP logging.	

* This parameter may not exist in some models.

config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer2 override-setting
    Description: Override FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
```

```

set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set use-management-vdom [enable|disable]

```

end

config log fortianalyzer2 override-setting

Parameter	Description	Type	Size								
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.				
Option	Description										
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.										
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35								
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.				
Option	Description										
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.										
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.		
Option	Description										
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.										

Parameter	Description	Type	Size
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option	Description	
	<i>sha256</i>	Use SHA256 as HMAC algorithm.	
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable IPS packet archive logging.	
	<i>disable</i>	Disable IPS packet archive logging.	
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
priority	Set log transmission priority.	option	-
	Option	Description	
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.	

Parameter	Description	Type	Size
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
server	The remote FortiAnalyzer.	string	Maximum length: 63
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63
ssl-min-proto- version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
status	Enable/disable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable logging to FortiAnalyzer.	
	<i>disable</i>	Disable logging to FortiAnalyzer.	
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option	Description	
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.	

Parameter	Description	Type	Size
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-

Option	Description
<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.
<i>realtime</i>	Log directly to FortiAnalyzer in real time.
<i>1-minute</i>	Log directly to FortiAnalyzer at most every 1 minute.
<i>5-minute</i>	Log directly to FortiAnalyzer at most every 5 minutes.

upload-time	Time to upload logs (hh:mm).	user	Not Specified
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-

Option	Description
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.

config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer2 setting
    Description: Global FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
```

```

set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
end

```

end

config log fortianalyzer2 setting

Parameter	Description	Type	Size								
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.				
Option	Description										
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.										
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35								
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.				
Option	Description										
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.										
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.		
Option	Description										
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.										
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-								

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td>sha1</td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	sha256	Use SHA256 as HMAC algorithm.	sha1	Step down to SHA1 as the HMAC algorithm.				
	Option	Description									
	sha256	Use SHA256 as HMAC algorithm.									
sha1	Step down to SHA1 as the HMAC algorithm.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.		
	Option	Description									
	auto	Set outgoing interface automatically.									
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.									
specify	Set outgoing interface manually.										
ips-archive	Enable/disable IPS packet archive logging.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS packet archive logging.</td></tr><tr><td>disable</td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	enable	Enable IPS packet archive logging.	disable	Disable IPS packet archive logging.				
	Option	Description									
	enable	Enable IPS packet archive logging.									
disable	Disable IPS packet archive logging.										
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400								
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120								
priority	Set log transmission priority.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.				
	Option	Description									
	default	Set FortiAnalyzer log transmission priority to default.									
low	Set FortiAnalyzer log transmission priority to low.										
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
server	The remote FortiAnalyzer.	string	Maximum length: 63
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
status	Enable/disable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable logging to FortiAnalyzer.	
	<i>disable</i>	Disable logging to FortiAnalyzer.	
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option	Description	
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	
	<i>1-minute</i>	Log directly to FortiAnalyzer at most every 1 minute.	
	<i>5-minute</i>	Log directly to FortiAnalyzer at most every 5 minutes.	
upload-time	Time to upload logs (hh:mm).	user	Not Specified

config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer3 filter
  Description: Filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
end
```

config log fortianalyzer3 filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	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	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	

Parameter	Description	Type	Size
	Option	Description	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VoIP logging.	
	<i>disable</i>	Disable VoIP logging.	

* This parameter may not exist in some models.

config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer3 override-filter
  Description: Override filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
end
```

config log fortianalyzer3 override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	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	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VoIP logging.	
	<i>disable</i>	Disable VoIP logging.	

* This parameter may not exist in some models.

config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer3 override-setting
  Description: Override FortiAnalyzer settings.
  set access-config [enable|disable]
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
```

```

set enc-algorithm [high-medium|high|...]
set hmac-algorithm [sha256|sha1]
set interface {string}
set interface-select-method [auto|sdwan|...]
set ips-archive [enable|disable]
set max-log-rate {integer}
set monitor-failure-retry-period {integer}
set monitor-keepalive-period {integer}
set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set use-management-vdom [enable|disable]

```

end

config log fortianalyzer3 override-setting

Parameter	Description	Type	Size						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
Option	Description								
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.								
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.								
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35						
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
Option	Description								
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.								
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.								
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600						
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-						

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.		
	Option	Description									
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.									
	<i>high</i>	Encrypt logs using high encryption algorithms.									
<i>low</i>	Encrypt logs using all encryption algorithms.										
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.				
	Option	Description									
	<i>sha256</i>	Use SHA256 as HMAC algorithm.									
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
	Option	Description									
	<i>auto</i>	Set outgoing interface automatically.									
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.										
ips-archive	Enable/disable IPS packet archive logging.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.				
	Option	Description									
	<i>enable</i>	Enable IPS packet archive logging.									
<i>disable</i>	Disable IPS packet archive logging.										
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400								
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120								

Parameter	Description	Type	Size
priority	Set log transmission priority.	option	-
	Option	Description	
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.	
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79
server	The remote FortiAnalyzer.	string	Maximum length: 63
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63
ssl-min-proto- version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
status	Enable/disable logging to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable logging to FortiAnalyzer.	
	<i>disable</i>	Disable logging to FortiAnalyzer.	
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-
	Option	Description	
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	
	<i>1-minute</i>	Log directly to FortiAnalyzer at most every 1 minute.	
	<i>5-minute</i>	Log directly to FortiAnalyzer at most every 5 minutes.	
upload-time	Time to upload logs (hh:mm).	user	Not Specified
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-
	Option	Description	
	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	
	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	

config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer3 setting
  Description: Global FortiAnalyzer settings.
  set access-config [enable|disable]
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set hmac-algorithm [sha256|sha1]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set max-log-rate {integer}
```

```

set monitor-failure-retry-period {integer}
set monitor-keepalive-period {integer}
set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}

```

end

config log fortianalyzer3 setting

Parameter	Description	Type	Size								
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.				
Option	Description										
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.										
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35								
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.				
Option	Description										
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.										
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.		
Option	Description										
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.										

Parameter	Description	Type	Size								
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td>sha1</td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	sha256	Use SHA256 as HMAC algorithm.	sha1	Step down to SHA1 as the HMAC algorithm.				
Option	Description										
sha256	Use SHA256 as HMAC algorithm.										
sha1	Step down to SHA1 as the HMAC algorithm.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.		
Option	Description										
auto	Set outgoing interface automatically.										
sdwan	Set outgoing interface by SD-WAN or policy routing rules.										
specify	Set outgoing interface manually.										
ips-archive	Enable/disable IPS packet archive logging.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS packet archive logging.</td></tr><tr><td>disable</td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	enable	Enable IPS packet archive logging.	disable	Disable IPS packet archive logging.				
Option	Description										
enable	Enable IPS packet archive logging.										
disable	Disable IPS packet archive logging.										
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400								
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120								
priority	Set log transmission priority.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr></table>	Option	Description	default	Set FortiAnalyzer log transmission priority to default.						
Option	Description										
default	Set FortiAnalyzer log transmission priority to default.										

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	<i>low</i>	Set FortiAnalyzer log transmission priority to low.										
Option	Description														
<i>low</i>	Set FortiAnalyzer log transmission priority to low.														
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.								
Option	Description														
<i>enable</i>	Enable reliable logging to FortiAnalyzer.														
<i>disable</i>	Disable reliable logging to FortiAnalyzer.														
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79												
server	The remote FortiAnalyzer.	string	Maximum length: 63												
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.		
Option	Description														
<i>default</i>	Follow system global setting.														
<i>SSLv3</i>	SSLv3.														
<i>TLSv1</i>	TLSv1.														
<i>TLSv1-1</i>	TLSv1.1.														
<i>TLSv1-2</i>	TLSv1.2.														
status	Enable/disable logging to FortiAnalyzer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.								
Option	Description														
<i>enable</i>	Enable logging to FortiAnalyzer.														
<i>disable</i>	Disable logging to FortiAnalyzer.														
upload-day	Day of week (month) to upload logs.	user	Not Specified												
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr></table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.										
Option	Description														
<i>daily</i>	Upload log files to FortiAnalyzer once a day.														

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.						
	Option	Description											
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.											
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.												
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>store-and-upload</i></td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td><i>realtime</i></td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td><i>1-minute</i></td><td>Log directly to FortiAnalyzer at most every 1 minute.</td></tr><tr><td><i>5-minute</i></td><td>Log directly to FortiAnalyzer at most every 5 minutes.</td></tr></table>	Option	Description	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	<i>1-minute</i>	Log directly to FortiAnalyzer at most every 1 minute.	<i>5-minute</i>	Log directly to FortiAnalyzer at most every 5 minutes.		
	Option	Description											
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.											
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.											
	<i>1-minute</i>	Log directly to FortiAnalyzer at most every 1 minute.											
<i>5-minute</i>	Log directly to FortiAnalyzer at most every 5 minutes.												
upload-time	Time to upload logs (hh:mm).	user	Not Specified										

config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```

config log fortianalyzer-cloud filter
    Description: Filters for FortiAnalyzer Cloud.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end

```

config log fortianalyzer-cloud filter

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

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	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	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VoIP logging.	
	<i>disable</i>	Disable VoIP logging.	

* This parameter may not exist in some models.

config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud override-filter
  Description: Override filters for FortiAnalyzer Cloud.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
```

```

set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]

```

end

config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
dlp-archive	Enable/disable DLP archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable DLP archive logging.	
	<i>disable</i>	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	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-
	Option	Description	
	<i>enable</i>	Enable VoIP logging.	
	<i>disable</i>	Disable VoIP logging.	

* This parameter may not exist in some models.

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	
	<i>enable</i>	Enable logging to FortiAnalyzer.	
	<i>disable</i>	Disable logging to FortiAnalyzer.	

config log fortianalyzer-cloud setting

Global FortiAnalyzer Cloud settings.

```

config log fortianalyzer-cloud setting
    Description: Global FortiAnalyzer Cloud settings.
    set access-config [enable|disable]
    set certificate {string}
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set priority [default|low]
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end

```

config log fortianalyzer-cloud setting

Parameter	Description	Type	Size
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-
	Option	Description	
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.	
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-
	Option	Description	
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	
	<i>high</i>	Encrypt logs using high encryption algorithms.	
	<i>low</i>	Encrypt logs using all encryption algorithms.	
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-
	Option	Description	
	<i>sha256</i>	Use SHA256 as HMAC algorithm.	
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	

Parameter	Description	Type	Size
ips-archive	Enable/disable IPS packet archive logging.	option	-
	Option	Description	
	<i>enable</i>	Enable IPS packet archive logging.	
	<i>disable</i>	Disable IPS packet archive logging.	
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120
priority	Set log transmission priority.	option	-
	Option	Description	
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
status	Enable/disable logging to FortiAnalyzer.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable logging to FortiAnalyzer.	
	<i>disable</i>	Disable logging to FortiAnalyzer.	
upload-day	Day of week (month) to upload logs.	user	Not Specified
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-
	Option	Description	
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-
	Option	Description	
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.	
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.	
	<i>1-minute</i>	Log directly to FortiAnalyzer at most every 1 minute.	
	<i>5-minute</i>	Log directly to FortiAnalyzer at most every 5 minutes.	
upload-time	Time to upload logs (hh:mm).	user	Not Specified

config log fortiguard filter

Filters for FortiCloud.

```

config log fortiguard filter
    Description: Filters for FortiCloud.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end

```

config log fortiguard filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	FortiCloud log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.		
	Option	Description																			
	<i>emergency</i>	Emergency level.																			
	<i>alert</i>	Alert level.																			
	<i>critical</i>	Critical level.																			
	<i>error</i>	Error level.																			
	<i>warning</i>	Warning level.																			
	<i>notification</i>	Notification level.																			
	<i>information</i>	Information level.																			
<i>debug</i>	Debug level.																				
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.														
	Option	Description																			
	<i>enable</i>	Enable sniffer traffic logging.																			
<i>disable</i>	Disable sniffer traffic logging.																				
voip	Enable/disable VoIP logging.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.														
	Option	Description																			
	<i>enable</i>	Enable VoIP logging.																			
<i>disable</i>	Disable VoIP logging.																				

* This parameter may not exist in some models.

config log fortiguard override-filter

Override filters for FortiCloud.

```

config log fortiguard override-filter
    Description: Override filters for FortiCloud.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end

```

config log fortiguard override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	FortiCloud log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.		
	Option	Description																			
	<i>emergency</i>	Emergency level.																			
	<i>alert</i>	Alert level.																			
	<i>critical</i>	Critical level.																			
	<i>error</i>	Error level.																			
	<i>warning</i>	Warning level.																			
	<i>notification</i>	Notification level.																			
	<i>information</i>	Information level.																			
<i>debug</i>	Debug level.																				
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.														
	Option	Description																			
	<i>enable</i>	Enable sniffer traffic logging.																			
<i>disable</i>	Disable sniffer traffic logging.																				
voip	Enable/disable VoIP logging.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.														
	Option	Description																			
	<i>enable</i>	Enable VoIP logging.																			
<i>disable</i>	Disable VoIP logging.																				

* This parameter may not exist in some models.

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 max-log-rate {integer}
    set override [enable|disable]
    set priority [default|low]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end
```

config log fortiguard override-setting

Parameter	Description	Type	Size										
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000										
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override FortiCloud logging settings.</td></tr><tr><td>disable</td><td>Use global FortiCloud logging settings.</td></tr></table>	Option	Description	enable	Override FortiCloud logging settings.	disable	Use global FortiCloud logging settings.						
Option	Description												
enable	Override FortiCloud logging settings.												
disable	Use global FortiCloud logging settings.												
priority	Set log transmission priority.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiCloud log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiCloud log transmission priority to low.</td></tr></table>	Option	Description	default	Set FortiCloud log transmission priority to default.	low	Set FortiCloud log transmission priority to low.						
Option	Description												
default	Set FortiCloud log transmission priority to default.												
low	Set FortiCloud log transmission priority to low.												
status	Enable/disable logging to FortiCloud.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiCloud.</td></tr><tr><td>disable</td><td>Disable logging to FortiCloud.</td></tr></table>	Option	Description	enable	Enable logging to FortiCloud.	disable	Disable logging to FortiCloud.						
Option	Description												
enable	Enable logging to FortiCloud.												
disable	Disable logging to FortiCloud.												
upload-day	Day of week to roll logs.	user	Not Specified										
upload-interval	Frequency of uploading log files to FortiCloud.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiCloud once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiCloud once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiCloud once a month.</td></tr></table>	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.				
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-option	Configure how log messages are sent to FortiCloud.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to the hard disk and then upload logs to FortiCloud.</td></tr><tr><td>realtime</td><td>Log directly to FortiCloud in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiCloud at 1-minute intervals.</td></tr><tr><td>5-minute</td><td>Log directly to FortiCloud at 5-minute intervals.</td></tr></table>	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.		
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-time	Time of day to roll logs (hh:mm).	user	Not Specified

config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
    Description: Configure logging to FortiCloud.
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set priority [default|low]
    set source-ip {ipv4-address}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end
```

config log fortiguard setting

Parameter	Description	Type	Size								
conn-timeout	FortiGate Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>Encrypt logs using high and medium encryption.</td></tr><tr><td>high</td><td>Encrypt logs using high encryption.</td></tr><tr><td>low</td><td>Encrypt logs using low encryption.</td></tr></table>			Option	Description	high-medium	Encrypt logs using high and medium encryption.	high	Encrypt logs using high encryption.	low	Encrypt logs using low encryption.
	Option	Description									
	high-medium	Encrypt logs using high and medium encryption.									
	high	Encrypt logs using high encryption.									
low	Encrypt logs using low encryption.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
priority	Set log transmission priority.	option	-
	Option	Description	
	<i>default</i>	Set FortiCloud log transmission priority to default.	
	<i>low</i>	Set FortiCloud log transmission priority to low.	
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
status	Enable/disable logging to FortiCloud.	option	-
	Option	Description	
	<i>enable</i>	Enable logging to FortiCloud.	
	<i>disable</i>	Disable logging to FortiCloud.	
upload-day	Day of week to roll logs.	user	Not Specified
upload-interval	Frequency of uploading log files to FortiCloud.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>daily</i>	Upload log files to FortiCloud once a day.	
	<i>weekly</i>	Upload log files to FortiCloud once a week.	
	<i>monthly</i>	Upload log files to FortiCloud once a month.	
upload-option	Configure how log messages are sent to FortiCloud.	option	-
	Option	Description	
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.	
	<i>realtime</i>	Log directly to FortiCloud in real time.	
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.	
	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.	
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified

config log gui-display

Configure how log messages are displayed on the GUI.

```
config log gui-display
    Description: Configure how log messages are displayed on the GUI.
    set fortiview-unscanned-apps [enable|disable]
    set resolve-apps [enable|disable]
    set resolve-hosts [enable|disable]
end
```

config log gui-display

Parameter	Description	Type	Size						
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable showing unscanned traffic.</td></tr><tr><td><i>disable</i></td><td>Disable showing unscanned traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable showing unscanned traffic.	<i>disable</i>	Disable showing unscanned traffic.		
Option	Description								
<i>enable</i>	Enable showing unscanned traffic.								
<i>disable</i>	Disable showing unscanned traffic.								
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable unknown applications on the GUI.	
	<i>disable</i>	Disable unknown applications on the GUI.	
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup	option	-
	Option	Description	
	<i>enable</i>	Enable resolving IP addresses to hostnames.	
	<i>disable</i>	Disable resolving IP addresses to hostnames.	

config log memory filter

Filters for memory buffer.

```
config log memory filter
    Description: Filters for memory buffer.
    set admin [enable|disable]
    set anomaly [enable|disable]
    set auth [enable|disable]
    set chassis-loadbalance-ha [enable|disable]
    set cpu-memory-usage [enable|disable]
    set dhcp [enable|disable]
    set event [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set ha [enable|disable]
    set ipsec [enable|disable]
    set ldb-monitor [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set pattern [enable|disable]
    set ppp [enable|disable]
    set radius [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set sslvpn-log-adm [enable|disable]
    set sslvpn-log-auth [enable|disable]
    set sslvpn-log-session [enable|disable]
    set system [enable|disable]
    set vip-ssl [enable|disable]
    set voip [enable|disable]
    set wan-opt [enable|disable]
    set wireless-activity [enable|disable]
end
```

config log memory filter

Parameter	Description	Type	Size						
admin	Enable/disable admin login/logout logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable admin login/logout logging.</td></tr><tr><td><i>disable</i></td><td>Disable admin login/logout logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable admin login/logout logging.	<i>disable</i>	Disable admin login/logout logging.		
Option	Description								
<i>enable</i>	Enable admin login/logout logging.								
<i>disable</i>	Disable admin login/logout logging.								
anomaly	Enable/disable anomaly logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.		
Option	Description								
<i>enable</i>	Enable anomaly logging.								
<i>disable</i>	Disable anomaly logging.								
auth	Enable/disable firewall authentication logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable firewall authentication logging.</td></tr><tr><td><i>disable</i></td><td>Disable firewall authentication logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable firewall authentication logging.	<i>disable</i>	Disable firewall authentication logging.		
Option	Description								
<i>enable</i>	Enable firewall authentication logging.								
<i>disable</i>	Disable firewall authentication logging.								
chassis-loadbalance-ha *	Enable/disable chassis load balancer state changes logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable chassis load balancer state changes logging.</td></tr><tr><td><i>disable</i></td><td>Disable chassis load balancer state changes logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable chassis load balancer state changes logging.	<i>disable</i>	Disable chassis load balancer state changes logging.		
Option	Description								
<i>enable</i>	Enable chassis load balancer state changes logging.								
<i>disable</i>	Disable chassis load balancer state changes logging.								
cpu-memory-usage	Enable/disable CPU & memory usage logging every 5 minutes.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable CPU & memory usage logging every 5 minutes.</td></tr><tr><td><i>disable</i></td><td>Disable CPU & memory usage logging every 5 minutes.</td></tr></table>	Option	Description	<i>enable</i>	Enable CPU & memory usage logging every 5 minutes.	<i>disable</i>	Disable CPU & memory usage logging every 5 minutes.		
Option	Description								
<i>enable</i>	Enable CPU & memory usage logging every 5 minutes.								
<i>disable</i>	Disable CPU & memory usage logging every 5 minutes.								
dhcp	Enable/disable DHCP service messages logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP service messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP service messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP service messages logging.	<i>disable</i>	Disable DHCP service messages logging.		
Option	Description								
<i>enable</i>	Enable DHCP service messages logging.								
<i>disable</i>	Disable DHCP service messages logging.								

Parameter	Description	Type	Size
event	Enable/disable event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
filter	Memory log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
ha	Enable/disable HA logging.	option	-
	Option	Description	
	<i>enable</i>	Enable HA logging.	
	<i>disable</i>	Disable HA logging.	
ipsec	Enable/disable IPsec negotiation messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable IPsec negotiation messages logging.	
	<i>disable</i>	Disable IPsec negotiation messages logging.	
ldb-monitor	Enable/disable VIP real server health monitoring logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable VIP real server health monitoring logging.	
	<i>disable</i>	Disable VIP real server health monitoring logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
pattern	Enable/disable pattern update logging.	option	-
	Option	Description	
	<i>enable</i>	Enable pattern update logging.	
	<i>disable</i>	Disable pattern update logging.	
ppp	Enable/disable L2TP/PPTP/PPPoE logging.	option	-
	Option	Description	
	<i>enable</i>	Enable L2TP/PPTP/PPPoE logging.	
	<i>disable</i>	Disable L2TP/PPTP/PPPoE logging.	
radius	Enable/disable RADIUS messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable RADIUS messages logging.	
	<i>disable</i>	Disable RADIUS messages logging.	
severity	Log every message above and including this severity level.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	

Parameter	Description	Type	Size
	Option	Description	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sslvpn-log-adm	Enable/disable SSL administrator login logging.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL administrator logging.	
	<i>disable</i>	Disable SSL administrator logging.	
sslvpn-log-auth	Enable/disable SSL user authentication logging.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL user authentication logging.	
	<i>disable</i>	Disable SSL user authentication logging.	
sslvpn-log-session	Enable/disable SSL session logging.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL session logging.	
	<i>disable</i>	Disable SSL session logging.	
system	Enable/disable system activity logging.	option	-
	Option	Description	
	<i>enable</i>	Enable system activity logging.	
	<i>disable</i>	Disable system activity logging.	

Parameter	Description	Type	Size						
vip-ssl *	Enable/disable VIP SSL logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VIP SSL logging.</td></tr><tr><td><i>disable</i></td><td>Disable VIP SSL logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VIP SSL logging.	<i>disable</i>	Disable VIP SSL logging.		
Option	Description								
<i>enable</i>	Enable VIP SSL logging.								
<i>disable</i>	Disable VIP SSL logging.								
voip	Enable/disable VoIP logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.		
Option	Description								
<i>enable</i>	Enable VoIP logging.								
<i>disable</i>	Disable VoIP logging.								
wan-opt	Enable/disable WAN optimization event logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN optimization event logging.</td></tr><tr><td><i>disable</i></td><td>Disable WAN optimization event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable WAN optimization event logging.	<i>disable</i>	Disable WAN optimization event logging.		
Option	Description								
<i>enable</i>	Enable WAN optimization event logging.								
<i>disable</i>	Disable WAN optimization event logging.								
wireless-activity	Enable/disable wireless activity event logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless activity event logging.</td></tr><tr><td><i>disable</i></td><td>Disable wireless activity event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable wireless activity event logging.	<i>disable</i>	Disable wireless activity event logging.		
Option	Description								
<i>enable</i>	Enable wireless activity event logging.								
<i>disable</i>	Disable wireless activity event logging.								

* This parameter may not exist in some models.

config log memory global-setting

Global settings for memory logging.

```
config log memory global-setting
    Description: Global settings for memory logging.
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set max-size {integer}
end
```

config log memory global-setting

Parameter	Description	Type	Size
full-final-warning-threshold	Log full final warning threshold as a percent (3 - 100, default = 95).	integer	Minimum value: 3 Maximum value: 100
full-first-warning-threshold	Log full first warning threshold as a percent (1 - 98, default = 75).	integer	Minimum value: 1 Maximum value: 98
full-second-warning-threshold	Log full second warning threshold as a percent (2 - 99, default = 90).	integer	Minimum value: 2 Maximum value: 99
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295

config log memory setting

Settings for memory buffer.

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

config log memory setting

Parameter	Description	Type	Size				
diskfull	Action to take when memory is full.	option	-				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>overwrite</i></td><td>Overwrite the oldest logs when the system memory reserved for logging is full.</td></tr></table>			Option	Description	<i>overwrite</i>	Overwrite the oldest logs when the system memory reserved for logging is full.
Option	Description						
<i>overwrite</i>	Overwrite the oldest logs when the system memory reserved for logging is full.						
status	Enable/disable logging to the FortiGate's memory.	option	-				

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable logging to memory.	
	<i>disable</i>	Disable logging to memory.	

config log null-device filter

Filters for null device logging.

```
config log null-device filter
    Description: Filters for null device logging.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log null-device filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Null-device log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

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

* This parameter may not exist in some models.

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

config log setting

Configure general log settings.

```
config log setting
    Description: Configure general log settings.
```

```

set brief-traffic-format [enable|disable]
set custom-log-fields <field-id1>, <field-id2>, ...
set daemon-log [enable|disable]
set expolicy-implicit-log [enable|disable]
set faz-override [enable|disable]
set fortiview-weekly-data [enable|disable]
set fwpolicy-implicit-log [enable|disable]
set fwpolicy6-implicit-log [enable|disable]
set local-in-allow [enable|disable]
set local-in-deny-broadcast [enable|disable]
set local-in-deny-unicast [enable|disable]
set local-out [enable|disable]
set log-invalid-packet [enable|disable]
set log-policy-comment [enable|disable]
set log-policy-name [enable|disable]
set log-user-in-upper [enable|disable]
set neighbor-event [enable|disable]
set resolve-ip [enable|disable]
set resolve-port [enable|disable]
set syslog-override [enable|disable]
set user-anonymize [enable|disable]

```

end

config log setting

Parameter	Description	Type	Size						
brief-traffic-format	Enable/disable brief format traffic logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable brief format traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable brief format traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable brief format traffic logging.	<i>disable</i>	Disable brief format traffic logging.		
Option	Description								
<i>enable</i>	Enable brief format traffic logging.								
<i>disable</i>	Disable brief format traffic logging.								
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35						
daemon-log	Enable/disable daemon logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable daemon logging.</td></tr><tr><td><i>disable</i></td><td>Disable daemon logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable daemon logging.	<i>disable</i>	Disable daemon logging.		
Option	Description								
<i>enable</i>	Enable daemon logging.								
<i>disable</i>	Disable daemon logging.								
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable explicit proxy firewall implicit policy logging.	
	<i>disable</i>	Disable explicit proxy firewall implicit policy logging.	
faz-override	Enable/disable override FortiAnalyzer settings.	option	-
	Option	Description	
	<i>enable</i>	Enable override FortiAnalyzer settings.	
	<i>disable</i>	Disable override FortiAnalyzer settings.	
fortiview-weekly-data *	Enable/disable FortiView weekly data.	option	-
	Option	Description	
	<i>enable</i>	Enable FortiView weekly data.	
	<i>disable</i>	Disable FortiView weekly data.	
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-
	Option	Description	
	<i>enable</i>	Enable implicit firewall policy logging.	
	<i>disable</i>	Disable implicit firewall policy logging.	
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-
	Option	Description	
	<i>enable</i>	Enable implicit firewall policy6 logging.	
	<i>disable</i>	Disable implicit firewall policy6 logging.	
local-in-allow	Enable/disable local-in-allow logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local-in-allow logging.	
	<i>disable</i>	Disable local-in-allow logging.	
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable local-in-deny-broadcast logging.	
	<i>disable</i>	Disable local-in-deny-broadcast logging.	
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local-in-deny-unicast logging.	
	<i>disable</i>	Disable local-in-deny-unicast logging.	
local-out	Enable/disable local-out logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local-out logging.	
	<i>disable</i>	Disable local-out logging.	
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable invalid packet traffic logging.	
	<i>disable</i>	Disable invalid packet traffic logging.	
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-
	Option	Description	
	<i>enable</i>	Enable inserting policy comments into traffic logs.	
	<i>disable</i>	Disable inserting policy comments into traffic logs.	
log-policy-name	Enable/disable inserting policy name into traffic logs.	option	-
	Option	Description	
	<i>enable</i>	Enable inserting policy name into traffic logs.	
	<i>disable</i>	Disable inserting policy name into traffic logs.	
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable logs with user-in-upper.	
	<i>disable</i>	Disable logs with user-in-upper.	
neighbor-event	Enable/disable neighbor event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable neighbor event logging.	
	<i>disable</i>	Disable neighbor event logging.	
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-
	Option	Description	
	<i>enable</i>	Enable adding resolved domain names to traffic logs.	
	<i>disable</i>	Disable adding resolved domain names to traffic logs.	
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-
	Option	Description	
	<i>enable</i>	Enable adding resolved service names to traffic logs.	
	<i>disable</i>	Disable adding resolved service names to traffic logs.	
syslog-override	Enable/disable override Syslog settings.	option	-
	Option	Description	
	<i>enable</i>	Enable override Syslog settings.	
	<i>disable</i>	Disable override Syslog settings.	
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-
	Option	Description	
	<i>enable</i>	Enable anonymizing user names in log messages.	
	<i>disable</i>	Disable anonymizing user names in log messages.	

* This parameter may not exist in some models.

config log syslogd filter

Filters for remote system server.

```
config log syslogd filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd override-filter

Override filters for remote system server.

```
config log syslogd override-filter
    Description: Override filters for remote system server.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd override-setting

Override settings for remote syslog server.

```

config log syslogd override-setting
    Description: Override settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```


config log syslogd override-setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.		
	Option	Description															
	<i>local2</i>	Reserved for local use.															
	<i>local3</i>	Reserved for local use.															
	<i>local4</i>	Reserved for local use.															
	<i>local5</i>	Reserved for local use.															
	<i>local6</i>	Reserved for local use.															
<i>local7</i>	Reserved for local use.																
format	Log format.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.								
	Option	Description															
	<i>default</i>	Syslog format.															
	<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.																
interface	Specify outgoing interface to reach server.	string	Maximum length: 15														
interface-select-method	Specify how to select outgoing interface to reach server.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.								
	Option	Description															
	<i>auto</i>	Set outgoing interface automatically.															
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.																
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000														
mode	Remote syslog logging over UDP/Reliable TCP.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).								
	Option	Description															
	<i>udp</i>	Enable syslogging over UDP.															
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																

Parameter	Description	Type	Size
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
priority	Set log transmission priority.	option	-

Option	Description

<i>default</i>	Set Syslog transmission priority to default.

<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63
source-ip	Source IP address of syslog.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description

<i>default</i>	Follow system global setting.

<i>SSLv3</i>	SSLv3.

<i>TLSv1</i>	TLSv1.

<i>TLSv1-1</i>	TLSv1.1.

<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

Option	Description

<i>enable</i>	Log to remote syslog server.

<i>disable</i>	Do not log to remote syslog server.

config custom-field-name

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

Parameter	Description	Type	Size
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field name.	string	Maximum length: 35

config log syslogd setting

Global settings for remote syslog server.

```

config log syslogd setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```

config log syslogd setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>local6</td><td>Reserved for local use.</td></tr><tr><td>local7</td><td>Reserved for local use.</td></tr></table>	Option	Description	local6	Reserved for local use.	local7	Reserved for local use.				
	Option	Description									
	local6	Reserved for local use.									
local7	Reserved for local use.										
format	Log format.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Syslog format.</td></tr><tr><td>csv</td><td>CSV (Comma Separated Values) format.</td></tr><tr><td>cef</td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	default	Syslog format.	csv	CSV (Comma Separated Values) format.	cef	CEF (Common Event Format) format.		
	Option	Description									
	default	Syslog format.									
	csv	CSV (Comma Separated Values) format.									
cef	CEF (Common Event Format) format.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.		
	Option	Description									
	auto	Set outgoing interface automatically.									
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.									
specify	Set outgoing interface manually.										
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
	Option	Description									
	udp	Enable syslogging over UDP.									
	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).									
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).										
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535								

Parameter	Description	Type	Size
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63

source-ip	Source IP address of syslog.	string	Maximum length: 63

ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

Parameter	Description	Type	Size
custom	Field custom name.	string	Maximum length: 35
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field 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 anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd2 filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog 2 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
    Description: Override filters for remote system server.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd2 override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog 2 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd2 override-setting

Override settings for remote syslog server.

```
config log syslogd2 override-setting
    Description: Override settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end
```

config log syslogd2 override-setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.		
	Option	Description															
	<i>local2</i>	Reserved for local use.															
	<i>local3</i>	Reserved for local use.															
	<i>local4</i>	Reserved for local use.															
	<i>local5</i>	Reserved for local use.															
	<i>local6</i>	Reserved for local use.															
<i>local7</i>	Reserved for local use.																
format	Log format.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.								
	Option	Description															
	<i>default</i>	Syslog format.															
	<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.																
interface	Specify outgoing interface to reach server.	string	Maximum length: 15														
interface-select-method	Specify how to select outgoing interface to reach server.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.								
	Option	Description															
	<i>auto</i>	Set outgoing interface automatically.															
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.																
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000														
mode	Remote syslog logging over UDP/Reliable TCP.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).								
	Option	Description															
	<i>udp</i>	Enable syslogging over UDP.															
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																

Parameter	Description	Type	Size
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63
source-ip	Source IP address of syslog.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

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

Parameter	Description	Type	Size
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field name.	string	Maximum length: 35

config log syslogd2 setting

Global settings for remote syslog server.

```

config log syslogd2 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```

config log syslogd2 setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.				
	Option	Description									
	<i>local6</i>	Reserved for local use.									
<i>local7</i>	Reserved for local use.										
format	Log format.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.		
	Option	Description									
	<i>default</i>	Syslog format.									
	<i>csv</i>	CSV (Comma Separated Values) format.									
<i>cef</i>	CEF (Common Event Format) format.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
	Option	Description									
	<i>auto</i>	Set outgoing interface automatically.									
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.										
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
	Option	Description									
	<i>udp</i>	Enable syslogging over UDP.									
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).									
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).										
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535								

Parameter	Description	Type	Size
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63

source-ip	Source IP address of syslog.	string	Maximum length: 63

ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

Parameter	Description	Type	Size
custom	Field custom name.	string	Maximum length: 35
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field 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 anomaly [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
end
```

config log syslogd3 filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog 3 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd3 override-filter

Override filters for remote system server.

```
config log syslogd3 override-filter
    Description: Override filters for remote system server.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd3 override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog 3 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd3 override-setting

Override settings for remote syslog server.

```

config log syslogd3 override-setting
    Description: Override settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```


config log syslogd3 override-setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.		
	Option	Description															
	<i>local2</i>	Reserved for local use.															
	<i>local3</i>	Reserved for local use.															
	<i>local4</i>	Reserved for local use.															
	<i>local5</i>	Reserved for local use.															
	<i>local6</i>	Reserved for local use.															
<i>local7</i>	Reserved for local use.																
format	Log format.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.								
	Option	Description															
	<i>default</i>	Syslog format.															
	<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.																
interface	Specify outgoing interface to reach server.	string	Maximum length: 15														
interface-select-method	Specify how to select outgoing interface to reach server.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.								
	Option	Description															
	<i>auto</i>	Set outgoing interface automatically.															
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.																
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000														
mode	Remote syslog logging over UDP/Reliable TCP.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).								
	Option	Description															
	<i>udp</i>	Enable syslogging over UDP.															
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																

Parameter	Description	Type	Size
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63
source-ip	Source IP address of syslog.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

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

Parameter	Description	Type	Size
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field name.	string	Maximum length: 35

config log syslogd3 setting

Global settings for remote syslog server.

```

config log syslogd3 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```

config log syslogd3 setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.				
	Option	Description									
	<i>local6</i>	Reserved for local use.									
<i>local7</i>	Reserved for local use.										
format	Log format.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.		
	Option	Description									
	<i>default</i>	Syslog format.									
	<i>csv</i>	CSV (Comma Separated Values) format.									
<i>cef</i>	CEF (Common Event Format) format.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
	Option	Description									
	<i>auto</i>	Set outgoing interface automatically.									
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.										
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
	Option	Description									
	<i>udp</i>	Enable syslogging over UDP.									
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).									
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).										
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535								

Parameter	Description	Type	Size
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63

source-ip	Source IP address of syslog.	string	Maximum length: 63

ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

Parameter	Description	Type	Size
custom	Field custom name.	string	Maximum length: 35
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field 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 anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd4 filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog 4 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd4 override-filter

Override filters for remote system server.

```
config log syslogd4 override-filter
    Description: Override filters for remote system server.
    set anomaly [enable|disable]
    set filter {string}
    set filter-type [include|exclude]
    set forward-traffic [enable|disable]
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
end
```

config log syslogd4 override-filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Syslog 4 filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	

Parameter	Description	Type	Size
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-

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

* This parameter may not exist in some models.

config log syslogd4 override-setting

Override settings for remote syslog server.

```

config log syslogd4 override-setting
    Description: Override settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```

config log syslogd4 override-setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.		
	Option	Description															
	<i>local2</i>	Reserved for local use.															
	<i>local3</i>	Reserved for local use.															
	<i>local4</i>	Reserved for local use.															
	<i>local5</i>	Reserved for local use.															
	<i>local6</i>	Reserved for local use.															
<i>local7</i>	Reserved for local use.																
format	Log format.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.								
	Option	Description															
	<i>default</i>	Syslog format.															
	<i>csv</i>	CSV (Comma Separated Values) format.															
<i>cef</i>	CEF (Common Event Format) format.																
interface	Specify outgoing interface to reach server.	string	Maximum length: 15														
interface-select-method	Specify how to select outgoing interface to reach server.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.								
	Option	Description															
	<i>auto</i>	Set outgoing interface automatically.															
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.															
<i>specify</i>	Set outgoing interface manually.																
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000														
mode	Remote syslog logging over UDP/Reliable TCP.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).								
	Option	Description															
	<i>udp</i>	Enable syslogging over UDP.															
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).															
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																

Parameter	Description	Type	Size
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63
source-ip	Source IP address of syslog.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

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

Parameter	Description	Type	Size
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field name.	string	Maximum length: 35

config log syslogd4 setting

Global settings for remote syslog server.

```

config log syslogd4 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end

```

config log syslogd4 setting

Parameter	Description	Type	Size
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-

Parameter	Description	Type	Size

Option	Description
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.
<i>high</i>	SSL communication with high encryption algorithms.
<i>low</i>	SSL communication with low encryption algorithms.
<i>disable</i>	Disable SSL communication.

facility	Remote syslog facility.	option	-

Option	Description
<i>kernel</i>	Kernel messages.
<i>user</i>	Random user-level messages.
<i>mail</i>	Mail system.
<i>daemon</i>	System daemons.
<i>auth</i>	Security/authorization messages.
<i>syslog</i>	Messages generated internally by syslog.
<i>lpr</i>	Line printer subsystem.
<i>news</i>	Network news subsystem.
<i>uucp</i>	Network news subsystem.
<i>cron</i>	Clock daemon.
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.

Parameter	Description	Type	Size
	Option	Description	
	<i>local6</i>	Reserved for local use.	
	<i>local7</i>	Reserved for local use.	
format	Log format.	option	-
	Option	Description	
	<i>default</i>	Syslog format.	
	<i>csv</i>	CSV (Comma Separated Values) format.	
	<i>cef</i>	CEF (Common Event Format) format.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000
mode	Remote syslog logging over UDP/Reliable TCP.	option	-
	Option	Description	
	<i>udp</i>	Enable syslogging over UDP.	
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).	
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
priority	Set log transmission priority.	option	-

Option	Description
<i>default</i>	Set Syslog transmission priority to default.
<i>low</i>	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 63

source-ip	Source IP address of syslog.	string	Maximum length: 63

ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

status	Enable/disable remote syslog logging.	option	-

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

config custom-field-name

Parameter	Description	Type	Size
custom	Field custom name.	string	Maximum length: 35
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
name	Field name.	string	Maximum length: 35

config log threat-weight

Configure threat weight settings.

```
config log threat-weight
  Description: Configure threat weight settings.
  config application
    Description: Application-control threat weight settings.
    edit <id>
      set category {integer}
      set level [disable|low|...]
    next
  end
  set blocked-connection [disable|low|...]
  set botnet-connection-detected [disable|low|...]
  set failed-connection [disable|low|...]
  config geolocation
    Description: Geolocation-based threat weight settings.
    edit <id>
      set country {string}
      set level [disable|low|...]
    next
  end
  config ips
    Description: IPS threat weight settings.
    set critical-severity [disable|low|...]
    set high-severity [disable|low|...]
    set info-severity [disable|low|...]
    set low-severity [disable|low|...]
    set medium-severity [disable|low|...]
  end
  config level
    Description: Score mapping for threat weight levels.
    set critical {integer}
    set high {integer}
    set low {integer}
    set medium {integer}
  end
  config malware
    Description: Anti-virus malware threat weight settings.
    set command-blocked [disable|low|...]
    set content-disarm [disable|low|...]
    set file-blocked [disable|low|...]
    set fsa-high-risk [disable|low|...]
    set fsa-malicious [disable|low|...]
    set fsa-medium-risk [disable|low|...]
    set malware-list [disable|low|...]
    set mimefragmented [disable|low|...]
    set oversized [disable|low|...]
    set switch-proto [disable|low|...]
    set virus-file-type-executable [disable|low|...]
    set virus-infected [disable|low|...]
    set virus-outbreak-prevention [disable|low|...]
    set virus-scan-error [disable|low|...]
  end
```

```

set status [enable|disable]
set url-block-detected [disable|low|...]
config web
    Description: Web filtering threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
end

```

config log threat-weight

Parameter	Description	Type	Size
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.	
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.	
failed-connection	Threat weight score for failed connections.	option	-
	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.	

Parameter	Description	Type	Size
	Option	Description	
	<i>high</i>	Use the high level score for failed connections.	
	<i>critical</i>	Use the critical level score for failed connections.	
status	Enable/disable the threat weight feature.	option	-
	Option	Description	
	<i>enable</i>	Enable the threat weight feature.	
	<i>disable</i>	Disable the threat weight feature.	
url-block-detected	Threat weight score for URL blocking.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for URL blocking.	
	<i>low</i>	Use the low level score for URL blocking.	
	<i>medium</i>	Use the medium level score for URL blocking.	
	<i>high</i>	Use the high level score for URL blocking.	
	<i>critical</i>	Use the critical level score for URL blocking.	

config application

Parameter	Description	Type	Size
category	Application category.	integer	Minimum value: 0 Maximum value: 65535
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
level	Threat weight score for Application events.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for Application events.	
	<i>low</i>	Use the low level score for Application events.	
	<i>medium</i>	Use the medium level score for Application events.	

Parameter	Description	Type	Size
	Option	Description	
	<i>high</i>	Use the high level score for Application events.	
	<i>critical</i>	Use the critical level score for Application events.	

config geolocation

Parameter	Description	Type	Size
country	Country code.	string	Maximum length: 2
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255
level	Threat weight score for Geolocation-based events.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.	
	<i>low</i>	Use the low level score for Geolocation-based events.	
	<i>medium</i>	Use the medium level score for Geolocation-based events.	
	<i>high</i>	Use the high level score for Geolocation-based events.	
	<i>critical</i>	Use the critical level score for Geolocation-based events.	

config ips

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

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

config level

Parameter	Description	Type	Size
critical	Critical level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100
high	High level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100
low	Low level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100
medium	Medium level score value (1 - 100).	integer	Minimum value: 1 Maximum value: 100

config malware

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

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>Use the high level score for virus (content disarm) detected.</td></tr><tr><td>critical</td><td>Use the critical level score for virus (content disarm) detected.</td></tr></table>	Option	Description	high	Use the high level score for virus (content disarm) detected.	critical	Use the critical level score for virus (content disarm) detected.								
	Option	Description													
	high	Use the high level score for virus (content disarm) detected.													
critical	Use the critical level score for virus (content disarm) detected.														
file-blocked	Threat weight score for blocked file detected.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for blocked file detected.</td></tr><tr><td>low</td><td>Use the low level score for blocked file detected.</td></tr><tr><td>medium</td><td>Use the medium level score for blocked file detected.</td></tr><tr><td>high</td><td>Use the high level score for blocked file detected.</td></tr><tr><td>critical</td><td>Use the critical level score for blocked file detected.</td></tr></table>	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.		
	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.														
fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for FortiSandbox high risk malware detected.</td></tr><tr><td>low</td><td>Use the low level score for FortiSandbox high risk malware detected.</td></tr><tr><td>medium</td><td>Use the medium level score for FortiSandbox high risk malware detected.</td></tr><tr><td>high</td><td>Use the high level score for FortiSandbox high risk malware detected.</td></tr><tr><td>critical</td><td>Use the critical level score for FortiSandbox high risk malware detected.</td></tr></table>	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.		
	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-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for FortiSandbox malicious malware detected.</td></tr><tr><td>low</td><td>Use the low level score for FortiSandbox malicious malware detected.</td></tr><tr><td>medium</td><td>Use the medium level score for FortiSandbox malicious malware detected.</td></tr><tr><td>high</td><td>Use the high level score for FortiSandbox malicious malware detected.</td></tr><tr><td>critical</td><td>Use the critical level score for FortiSandbox malicious malware detected.</td></tr></table>	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.		
	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-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-												

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

Parameter	Description	Type	Size
	Option	Description	
	<i>critical</i>	Use the critical level score for oversized file detected.	
switch-proto	Threat weight score for switch proto detected.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for switch proto detected.	
	<i>low</i>	Use the low level score for switch proto detected.	
	<i>medium</i>	Use the medium level score for switch proto detected.	
	<i>high</i>	Use the high level score for switch proto detected.	
	<i>critical</i>	Use the critical level score for switch proto detected.	
virus-file-type-executable	Threat weight score for virus (filetype executable) detected.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.	
	<i>low</i>	Use the low level score for virus (filetype executable) detected.	
	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.	
	<i>high</i>	Use the high level score for virus (filetype executable) detected.	
	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.	
virus-infected	Threat weight score for virus (infected) detected.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for virus (infected) detected.	
	<i>low</i>	Use the low level score for virus (infected) detected.	
	<i>medium</i>	Use the medium level score for virus (infected) detected.	
	<i>high</i>	Use the high level score for virus (infected) detected.	
	<i>critical</i>	Use the critical level score for virus (infected) detected.	
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.	

Parameter	Description	Type	Size
	Option	Description	
	<i>low</i>	Use the low level score for virus (outbreak prevention) event.	
	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.	
	<i>high</i>	Use the high level score for virus (outbreak prevention) event.	
	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.	
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-
	Option	Description	
	<i>disable</i>	Disable threat weight scoring for virus (scan error) detected.	
	<i>low</i>	Use the low level score for virus (scan error) detected.	
	<i>medium</i>	Use the medium level score for virus (scan error) detected.	
	<i>high</i>	Use the high level score for virus (scan error) detected.	
	<i>critical</i>	Use the critical level score for virus (scan error) detected.	

config web

Parameter	Description	Type	Size												
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255												
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255												
level	Threat weight score for web category filtering matches.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for web category filtering matches.</td></tr><tr><td>low</td><td>Use the low level score for web category filtering matches.</td></tr><tr><td>medium</td><td>Use the medium level score for web category filtering matches.</td></tr><tr><td>high</td><td>Use the high level score for web category filtering matches.</td></tr><tr><td>critical</td><td>Use the critical level score for web category filtering matches.</td></tr></table>			Option	Description	disable	Disable threat weight scoring for web category filtering matches.	low	Use the low level score for web category filtering matches.	medium	Use the medium level score for web category filtering matches.	high	Use the high level score for web category filtering matches.	critical	Use the critical level score for web category filtering matches.
Option	Description														
disable	Disable threat weight scoring for web category filtering matches.														
low	Use the low level score for web category filtering matches.														
medium	Use the medium level score for web category filtering matches.														
high	Use the high level score for web category filtering matches.														
critical	Use the critical level score for web category filtering matches.														

config log webtrends filter

Filters for WebTrends.

```
config log webtrends filter
  Description: Filters for WebTrends.
  set anomaly [enable|disable]
  set filter {string}
  set filter-type [include|exclude]
  set forward-traffic [enable|disable]
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
end
```

config log webtrends filter

Parameter	Description	Type	Size
anomaly	Enable/disable anomaly logging.	option	-
	Option	Description	
	<i>enable</i>	Enable anomaly logging.	
	<i>disable</i>	Disable anomaly logging.	
filter	Webtrends log filter.	string	Maximum length: 511
filter-type	Include/exclude logs that match the filter.	option	-
	Option	Description	
	<i>include</i>	Include logs that match the filter.	
	<i>exclude</i>	Exclude logs that match the filter.	
forward-traffic	Enable/disable forward traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable forward traffic logging.	
	<i>disable</i>	Disable forward traffic logging.	
gtp *	Enable/disable GTP messages logging.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP messages logging.	
	<i>disable</i>	Disable GTP messages logging.	
local-traffic	Enable/disable local in or out traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable local in or out traffic logging.	
	<i>disable</i>	Disable local in or out traffic logging.	
multicast-traffic	Enable/disable multicast traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable multicast traffic logging.	
	<i>disable</i>	Disable multicast traffic logging.	
severity	Lowest severity level to log to WebTrends.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer traffic logging.	
	<i>disable</i>	Disable sniffer traffic logging.	
voip	Enable/disable VoIP logging.	option	-

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

* This parameter may not exist in some models.

config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
    Description: Settings for WebTrends.
    set server {string}
    set status [enable|disable]
end
```

config log webtrends setting

Parameter	Description	Type	Size
server	Address of the remote WebTrends server.	string	Maximum length: 63
status	Enable/disable logging to WebTrends.	option	-
	Option	Description	
	<i>enable</i>	Enable logging to WebTrends.	
	<i>disable</i>	Disable logging to WebTrends.	

monitoring

This section includes syntax for the following commands:

- [config monitoring np6-ipsec-engine on page 577](#)
- [config monitoring npu-hpe on page 578](#)

config monitoring np6-ipsec-engine



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 201E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NP6 IPsec engine status monitoring.

```
config monitoring np6-ipsec-engine
    Description: Configure NP6 IPsec engine status monitoring.
    set interval {integer}
    set status [enable|disable]
    set threshold {user}
end
```

config monitoring np6-ipsec-engine

Parameter	Description	Type	Size						
interval	IPsec engine status check interval (1 - 60 seconds, default = 1).	integer	Minimum value: 1 Maximum value: 60						
status	Enable/disable NP6 IPsec engine status monitoring.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
threshold	IPsec engine status check threshold (x x x x x x x x, 8 integers from <1> to <255>, default = 15 15 12 12 8 8 5 5). Example: Log is generated if IPsec engine 0 is busy each of every 15 consecutive interval checks.	user	Not Specified						

config monitoring npu-hpe



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 201E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure npu-hpe status monitoring.

```

config monitoring npu-hpe
    Description: Configure npu-hpe status monitoring.
    set interval {integer}
    set multipliers {user}
    set status [enable|disable]
end

```

config monitoring npu-hpe

Parameter	Description	Type	Size
interval	HPE status check interval (1 - 60 seconds, default = 1 second).	integer	Minimum value: 1 Maximum value: 60
multipliers	HPE type interval multipliers (12 integers from <1> to <255>, default = 4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8). An event log is generated after every (interval * multiplier)seconds as configured for any HPE type when drops occur for that HPE type. An attack log is generated after every (4 * multiplier) number of continuous event logs.	user	Not Specified
status	Enable/disable HPE status monitoring.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

report

This section includes syntax for the following commands:

- [config report chart on page 580](#)
- [config report dataset on page 590](#)
- [config report layout on page 592](#)
- [config report setting on page 602](#)
- [config report style on page 604](#)
- [config report theme on page 608](#)

config report chart



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report chart widget configuration.

```
config report chart
  Description: Report chart widget configuration.
  edit <name>
    set background {string}
    set category [misc|traffic|...]
```

```

config category-series
    Description: Category series of pie chart.
    set databind {string}
    set font-size {integer}
end
set color-palette {string}
config column
    Description: Table column definition.
    edit <id>
        set detail-unit {string}
        set detail-value {string}
        set footer-unit {string}
        set footer-value {string}
        set header-value {string}
        config mapping
            Description: Show detail in certain display value for certain condition.
            edit <id>
                set displayname {string}
                set op [none|greater|...]
                set value-type [integer|string]
                set value1 {string}
                set value2 {string}
            next
        end
    next
end
set comments {string}
set dataset {string}
set dimension [2D|3D]
config drill-down-charts
    Description: Drill down charts.
    edit <id>
        set chart-name {string}
        set status [enable|disable]
    next
end
set favorite [no|yes]
set graph-type [none|bar|...]
set legend [enable|disable]
set legend-font-size {integer}
set period [last24h|last7d]
set policy {integer}
set style [auto|manual]
set title {string}
set title-font-size {integer}
set type [graph|table]
config value-series
    Description: Value series of pie chart.
    set databind {string}
end
config x-series
    Description: X-series of chart.
    set caption {string}
    set caption-font-size {integer}
    set databind {string}
    set font-size {integer}

```

```

        set is-category [yes|no]
        set label-angle [45-degree|vertical|...]
        set scale-direction [decrease|increase]
        set scale-format [YYYY-MM-DD-HH-MM|YYYY-MM-DD HH|...]
        set scale-step {integer}
        set scale-unit [minute|hour|...]
        set unit {string}
    end
    config y-series
        Description: Y-series of chart.
        set caption {string}
        set caption-font-size {integer}
        set databind {string}
        set extra-databind {string}
        set extra-y [enable|disable]
        set extra-y-legend {string}
        set font-size {integer}
        set group {string}
        set label-angle [45-degree|vertical|...]
        set unit {string}
        set y-legend {string}
    end
next
end

```

config report chart

Parameter	Description	Type	Size
background	Chart background.	string	Maximum length: 11
category	Category.	option	-

Option	Description
<i>misc</i>	Miscellaneous.
<i>traffic</i>	Traffic.
<i>event</i>	Event.
<i>virus</i>	Virus.
<i>webfilter</i>	Webfilter.
<i>attack</i>	Attack.
<i>spam</i>	Spam.
<i>dlp</i>	Data leak prevention.
<i>app-ctrl</i>	Application control.
<i>vulnerability</i>	Vulnerability.

Parameter	Description	Type	Size
color-palette	Color palette (system will pick color automatically by default).	string	Maximum length: 11
comments	Comment.	string	Maximum length: 127
dataset	Bind dataset to chart.	string	Maximum length: 71
dimension	Dimension.	option	-

Option	Description
<i>2D</i>	2D graphic.
<i>3D</i>	3D graphic.

favorite	Favorite.	option	-

Option	Description
<i>no</i>	Not a favorite chart.
<i>yes</i>	Favorite chart.

graph-type	Graph type.	option	-

Option	Description
<i>none</i>	None.
<i>bar</i>	Bar Chart.
<i>pie</i>	Pie Chart.
<i>line</i>	Line Chart.
<i>flow</i>	flow Chart.

legend	Enable/Disable Legend area.	option	-

Option	Description
<i>enable</i>	Enable legend area.
<i>disable</i>	Disable legend area.

legend-font-size	Font size of legend area.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size						
name	Chart Widget Name	string	Maximum length: 71						
period	Time period.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>last24h</i></td><td>Last 24 hours.</td></tr><tr><td><i>last7d</i></td><td>Last 7 days.</td></tr></table>	Option	Description	<i>last24h</i>	Last 24 hours.	<i>last7d</i>	Last 7 days.		
Option	Description								
<i>last24h</i>	Last 24 hours.								
<i>last7d</i>	Last 7 days.								
policy	Used by monitor policy. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295						
style	Style.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Auto.</td></tr><tr><td><i>manual</i></td><td>Manual.</td></tr></table>	Option	Description	<i>auto</i>	Auto.	<i>manual</i>	Manual.		
Option	Description								
<i>auto</i>	Auto.								
<i>manual</i>	Manual.								
title	Chart title.	string	Maximum length: 63						
title-font-size	Font size of chart title.	integer	Minimum value: 0 Maximum value: 4294967295						
type	Chart type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>graph</i></td><td>Graph.</td></tr><tr><td><i>table</i></td><td>Table.</td></tr></table>	Option	Description	<i>graph</i>	Graph.	<i>table</i>	Table.		
Option	Description								
<i>graph</i>	Graph.								
<i>table</i>	Table.								

config category-series

Parameter	Description	Type	Size
databind	Category series value expression.	string	Maximum length: 127
font-size	Font size of category-series title.	integer	Minimum value: 5 Maximum value: 20

config column

Parameter	Description	Type	Size
detail-unit	Detail unit of column.	string	Maximum length: 35
detail-value	Detail value of column.	string	Maximum length: 127
footer-unit	Footer unit of column.	string	Maximum length: 35
footer-value	Footer value of column.	string	Maximum length: 127
header-value	Display name of table header.	string	Maximum length: 127
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295

config mapping

Parameter	Description	Type	Size
displayname	Display name.	string	Maximum length: 127
id	id	integer	Minimum value: 0 Maximum value: 4294967295
op	Comparison operator.	option	-

Option	Description
<i>none</i>	None.
<i>greater</i>	Greater than.
<i>greater-equal</i>	Greater than or equal to.
<i>less</i>	Less than.
<i>less-equal</i>	Less than or equal to.
<i>equal</i>	Equal to.
<i>between</i>	Between value 1 and value 2.

Parameter	Description	Type	Size
value-type	Value type.	option	-
	Option	Description	
	<i>integer</i>	Integer.	
	<i>string</i>	String.	
value1	Value 1.	string	Maximum length: 127
value2	Value 2.	string	Maximum length: 127

config drill-down-charts

Parameter	Description	Type	Size
chart-name	Drill down chart name.	string	Maximum length: 71
id	Drill down chart ID.	integer	Minimum value: 0 Maximum value: 4294967295
status	Enable/disable this drill down chart.	option	-
	Option	Description	
	<i>enable</i>	Enable this drill down chart.	
	<i>disable</i>	Disable this drill down chart.	

config value-series

Parameter	Description	Type	Size
databind	Value series value expression.	string	Maximum length: 127

config x-series

Parameter	Description	Type	Size
caption	X-series caption.	string	Maximum length: 35

Parameter	Description	Type	Size
caption-font-size	X-series caption font size.	integer	Minimum value: 5 Maximum value: 20
databind	X-series value expression.	string	Maximum length: 127
font-size	X-series label font size.	integer	Minimum value: 5 Maximum value: 20
is-category	X-series represent category or not.	option	-

Option	Description
<i>yes</i>	X-series is category.
<i>no</i>	X-series is not category.

label-angle	X-series label angle.	option	-

Option	Description
<i>45-degree</i>	45-degree.
<i>vertical</i>	Vertical.
<i>horizontal</i>	Horizontal.

scale-direction	Scale increase or decrease.	option	-

Option	Description
<i>decrease</i>	Decrease.
<i>increase</i>	Increase.

scale-format	Date/time format.	option	-

Option	Description
<i>YYYY-MM-DD-HH-MM</i>	YYYY/MM/DD HH:MM
<i>YYYY-MM-DD HH</i>	YYYY/MM/DD HH
<i>YYYY-MM-DD</i>	YYYY/MM/DD
<i>YYYY-MM</i>	YYYY/MM

Parameter	Description	Type	Size
	Option	Description	
	YYYY	YYYY	
	HH-MM	HH:MM	
	MM-DD	MM:DD	
scale-step	Scale step.	integer	Minimum value: 1 Maximum value: 65535
scale-unit	Scale unit.	option	-
	Option	Description	
	<i>minute</i>	Minute.	
	<i>hour</i>	Hour.	
	<i>day</i>	Day.	
	<i>month</i>	Month.	
	<i>year</i>	Year.	
unit	X-series unit.	string	Maximum length: 35

config y-series

Parameter	Description	Type	Size
caption	Y-series caption.	string	Maximum length: 35
caption-font-size	Y-series caption font size.	integer	Minimum value: 5 Maximum value: 20
databind	Y-series value expression.	string	Maximum length: 127
extra-databind	Extra Y-series value.	string	Maximum length: 127
extra-y	Allow another Y-series value	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable second Y-series.	
	<i>disable</i>	Disable second Y-series.	
extra-y-legend	Extra Y-series legend type/name.	string	Maximum length: 35
font-size	Y-series label font size.	integer	Minimum value: 5 Maximum value: 20
group	Y-series group option.	string	Maximum length: 127
label-angle	Y-series label angle.	option	-
	Option	Description	
	<i>45-degree</i>	45-degree.	
	<i>vertical</i>	Vertical.	
	<i>horizontal</i>	Horizontal.	
unit	Y-series unit.	string	Maximum length: 35
y-legend	First Y-series legend type/name.	string	Maximum length: 35

config report dataset



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report dataset configuration.

```
config report dataset
  Description: Report dataset configuration.
  edit <name>
    config field
      Description: Fields.
      edit <id>
        set displayname {string}
        set name {string}
        set type [text|integer|...]
      next
    end
    config parameters
      Description: Parameters.
      edit <id>
        set data-type [text|integer|...]
        set display-name {string}
        set field {string}
      next
    end
    set policy {integer}
    set query {string}
  next
end
```

config report dataset

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 71
policy	Used by monitor policy. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
query	SQL query statement.	string	Maximum length: 2303

config field

Parameter	Description	Type	Size
displayname	Display name.	string	Maximum length: 127
id	Field ID (1 to number of columns in SQL result).	integer	Minimum value: 0 Maximum value: 4294967295
name	Name.	string	Maximum length: 71
type	Field type.	option	-

Option	Description
<i>text</i>	Text.
<i>integer</i>	Integer.
<i>double</i>	Double.

config parameters

Parameter	Description	Type	Size
data-type	Data type.	option	-

Option	Description
<i>text</i>	Text.

Parameter	Description	Type	Size
	Option	Description	
	<i>integer</i>	Integer.	
	<i>double</i>	Double.	
	<i>long-integer</i>	Long integer.	
	<i>date-time</i>	Date and time.	
display-name	Display name.	string	Maximum length: 127
field	SQL field name.	string	Maximum length: 127
id	Parameter ID (1 to number of columns in SQL result).	integer	Minimum value: 0 Maximum value: 4294967295

config report layout



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report layout configuration.

```
config report layout
  Description: Report layout configuration.
  edit <name>
    config body-item
      Description: Configure report body item.
      edit <id>
        set chart {string}
        set chart-options {option1}, {option2}, ...
        set column {integer}
        set content {string}
        set description {string}
        set drill-down-items {string}
        set drill-down-types {string}
        set hide [enable|disable]
        set img-src {string}
      config list
        Description: Configure report list item.
        edit <id>
          set content {string}
        next
      end
      set list-component [bullet|numbered]
      set misc-component [hline|page-break|...]
    config parameters
      Description: Parameters.
      edit <id>
        set name {string}
        set value {string}
      next
    end
    set style {string}
    set table-caption-style {string}
    set table-column-widths {string}
    set table-even-row-style {string}
    set table-head-style {string}
    set table-odd-row-style {string}
    set text-component [text|heading1|...]
    set title {string}
    set top-n {integer}
    set type [text|image|...]
  next
end
set cutoff-option [run-time|custom]
set cutoff-time {user}
set day [sunday|monday|...]
set description {string}
set email-recipients {string}
set email-send [enable|disable]
set format {option1}, {option2}, ...
set max-pdf-report {integer}
set options {option1}, {option2}, ...
config page
  Description: Configure report page.
  set column-break-before {option1}, {option2}, ...
config footer
```

```

Description: Configure report page footer.
config footer-item
    Description: Configure report footer item.
    edit <id>
        set content {string}
        set description {string}
        set img-src {string}
        set style {string}
        set type [text|image]
    next
end
set style {string}
end
config header
Description: Configure report page header.
config header-item
    Description: Configure report header item.
    edit <id>
        set content {string}
        set description {string}
        set img-src {string}
        set style {string}
        set type [text|image]
    next
end
set style {string}
end
set options {option1}, {option2}, ...
set page-break-before {option1}, {option2}, ...
set paper [a4|letter]
end
set schedule-type [demand|daily|...]
set style-theme {string}
set subtitle {string}
set time {user}
set title {string}
next
end

```

config report layout

Parameter	Description	Type	Size
cutoff-option	Cutoff-option is either run-time or custom.	option	-
	Option	Description	
	<i>run-time</i>	Run time.	
	<i>custom</i>	Custom.	
cutoff-time	Custom cutoff time to generate report [hh:mm].	user	Not Specified

Parameter	Description	Type	Size																
day	Schedule days of week to generate report.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>	Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.		
	Option	Description																	
	<i>sunday</i>	Sunday.																	
	<i>monday</i>	Monday.																	
	<i>tuesday</i>	Tuesday.																	
	<i>wednesday</i>	Wednesday.																	
	<i>thursday</i>	Thursday.																	
	<i>friday</i>	Friday.																	
<i>saturday</i>	Saturday.																		
description	Description.	string	Maximum length: 127																
email-recipients	Email recipients for generated reports.	string	Maximum length: 511																
email-send	Enable/disable sending emails after reports are generated.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending emails after generating reports.</td></tr><tr><td><i>disable</i></td><td>Disable sending emails after generating reports.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending emails after generating reports.	<i>disable</i>	Disable sending emails after generating reports.												
	Option	Description																	
	<i>enable</i>	Enable sending emails after generating reports.																	
<i>disable</i>	Disable sending emails after generating reports.																		
format	Report format.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pdf</i></td><td>PDF.</td></tr></table>	Option	Description	<i>pdf</i>	PDF.														
	Option	Description																	
<i>pdf</i>	PDF.																		
max-pdf-report	Maximum number of PDF reports to keep at one time (oldest report is overwritten).	integer	Minimum value: 1 Maximum value: 365																
name	Report layout name.	string	Maximum length: 35																
options	Report layout options.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include-table-of-content</i></td><td>Include table of content in the report.</td></tr></table>	Option	Description	<i>include-table-of-content</i>	Include table of content in the report.														
	Option	Description																	
<i>include-table-of-content</i>	Include table of content in the report.																		

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-numbering-heading</i></td><td>Prepend heading with auto numbering.</td></tr><tr><td><i>view-chart-as-heading</i></td><td>Auto add heading for each chart.</td></tr><tr><td><i>show-html-navbar-before-heading</i></td><td>Show HTML navigation bar before each heading.</td></tr><tr><td><i>dummy-option</i></td><td>Use this option if you need none of the above options.</td></tr></table>	Option	Description	<i>auto-numbering-heading</i>	Prepend heading with auto numbering.	<i>view-chart-as-heading</i>	Auto add heading for each chart.	<i>show-html-navbar-before-heading</i>	Show HTML navigation bar before each heading.	<i>dummy-option</i>	Use this option if you need none of the above options.		
	Option	Description											
	<i>auto-numbering-heading</i>	Prepend heading with auto numbering.											
	<i>view-chart-as-heading</i>	Auto add heading for each chart.											
	<i>show-html-navbar-before-heading</i>	Show HTML navigation bar before each heading.											
<i>dummy-option</i>	Use this option if you need none of the above options.												
schedule-type	Report schedule type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>demand</i></td><td>Run on demand.</td></tr><tr><td><i>daily</i></td><td>Schedule daily.</td></tr><tr><td><i>weekly</i></td><td>Schedule weekly.</td></tr></table>	Option	Description	<i>demand</i>	Run on demand.	<i>daily</i>	Schedule daily.	<i>weekly</i>	Schedule weekly.				
	Option	Description											
	<i>demand</i>	Run on demand.											
	<i>daily</i>	Schedule daily.											
<i>weekly</i>	Schedule weekly.												
style-theme	Report style theme.	string	Maximum length: 35										
subtitle	Report subtitle.	string	Maximum length: 127										
time	Schedule time to generate report [hh:mm].	user	Not Specified										
title	Report title.	string	Maximum length: 127										

config body-item

Parameter	Description	Type	Size
chart	Report item chart name.	string	Maximum length: 71
chart-options	Report chart options.	option	-
	OptionDescription		
	include-no-data	Include chart with no data.	
	hide-title	Hide chart title.	
	show-caption	Show chart caption.	

Parameter	Description	Type	Size						
column	Report section column number.	integer	Minimum value: 0 Maximum value: 4294967295						
content	Report item text content.	string	Maximum length: 511						
description	Description.	string	Maximum length: 63						
drill-down-items	Control how drill down charts are shown.	string	Maximum length: 11						
drill-down-types	Control whether keys from the parent being combined or not.	string	Maximum length: 7						
hide	Enable/disable hide item in report.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable hide item in report.</td></tr><tr><td><i>disable</i></td><td>Disable hide item in report.</td></tr></table>			Option	Description	<i>enable</i>	Enable hide item in report.	<i>disable</i>	Disable hide item in report.
	Option	Description							
	<i>enable</i>	Enable hide item in report.							
<i>disable</i>	Disable hide item in report.								
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295						
img-src	Report item image file name.	string	Maximum length: 127						
list-component	Report item list component.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bullet</i></td><td>Bullet list.</td></tr><tr><td><i>numbered</i></td><td>Numbered list.</td></tr></table>			Option	Description	<i>bullet</i>	Bullet list.	<i>numbered</i>	Numbered list.
	Option	Description							
	<i>bullet</i>	Bullet list.							
<i>numbered</i>	Numbered list.								
misc-component	Report item miscellaneous component.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hline</i></td><td>Horizontal line.</td></tr><tr><td><i>page-break</i></td><td>Page break.</td></tr></table>			Option	Description	<i>hline</i>	Horizontal line.	<i>page-break</i>	Page break.
	Option	Description							
	<i>hline</i>	Horizontal line.							
<i>page-break</i>	Page break.								

Parameter	Description	Type	Size

Option	Description
<i>column-break</i>	Column break.
<i>section-start</i>	Section start.

style	Report item style.	string	Maximum length: 71
table-caption-style	Table chart caption style.	string	Maximum length: 71
table-column-widths	Report item table column widths.	string	Maximum length: 179
table-even-row-style	Table chart even row style.	string	Maximum length: 71
table-head-style	Table chart head style.	string	Maximum length: 71
table-odd-row-style	Table chart odd row style.	string	Maximum length: 71
text-component	Report item text component.	option	-

Option	Description
<i>text</i>	Normal text.
<i>heading1</i>	Heading 1.
<i>heading2</i>	Heading 2.
<i>heading3</i>	Heading 3.

title	Report section title.	string	Maximum length: 511
top-n	Value of top.	integer	Minimum value: 0 Maximum value: 4294967295
type	Report item type.	option	-

Option	Description
<i>text</i>	Text.
<i>image</i>	Image.

Parameter	Description	Type	Size
	Option	Description	
	<i>chart</i>	Chart.	
	<i>misc</i>	Miscellaneous.	

config list

Parameter	Description	Type	Size
content	List entry content.	string	Maximum length: 127
id	List entry ID.	integer	Minimum value: 0 Maximum value: 4294967295

config parameters

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Field name that match field of parameters defined in dataset.	string	Maximum length: 127
value	Value to replace corresponding field of parameters defined in dataset.	string	Maximum length: 1023

config page

Parameter	Description	Type	Size
column-break-before	Report page auto column break before heading.	option	-
	Option	Description	
	<i>heading1</i>	Column break before heading 1.	
	<i>heading2</i>	Column break before heading 2.	
	<i>heading3</i>	Column break before heading 3.	

Parameter	Description	Type	Size
options	Report page options.	option	-
	Option	Description	
	<i>header-on-first-page</i>	Show header on first page.	
	<i>footer-on-first-page</i>	Show footer on first page.	
page-break-before	Report page auto page break before heading.	option	-
	Option	Description	
	<i>heading1</i>	Page break before heading 1.	
	<i>heading2</i>	Page break before heading 2.	
	<i>heading3</i>	Page break before heading 3.	
paper	Report page paper.	option	-
	Option	Description	
	<i>a4</i>	A4 paper.	
	<i>letter</i>	Letter paper.	

config footer

Parameter	Description	Type	Size
style	Report footer style.	string	Maximum length: 71

config footer-item

Parameter	Description	Type	Size
content	Report item text content.	string	Maximum length: 511
description	Description.	string	Maximum length: 63
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
img-src	Report item image file name.	string	Maximum length: 127
style	Report item style.	string	Maximum length: 71
type	Report item type.	option	-
	Option	Description	
	<i>text</i>	Text.	
	<i>image</i>	Image.	

config header

Parameter	Description	Type	Size
style	Report header style.	string	Maximum length: 71

config header-item

Parameter	Description	Type	Size
content	Report item text content.	string	Maximum length: 511
description	Description.	string	Maximum length: 63
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295
img-src	Report item image file name.	string	Maximum length: 127
style	Report item style.	string	Maximum length: 71
type	Report item type.	option	-
	Option	Description	
	<i>text</i>	Text.	
	<i>image</i>	Image.	

config report setting



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report setting configuration.

```
config report setting
    Description: Report setting configuration.
    set fortiview [enable|disable]
    set pdf-report [enable|disable]
    set report-source {option1}, {option2}, ...
    set top-n {integer}
    set web-browsing-threshold {integer}
end
```

config report setting

Parameter	Description	Type	Size
fortiview	Enable/disable historical FortiView.	option	-
	Option	Description	
	<i>enable</i>	Enable historical FortiView.	
	<i>disable</i>	Disable historical FortiView.	

Parameter	Description	Type	Size
pdf-report	Enable/disable PDF report.	option	-
	Option	Description	
	<i>enable</i>	Enable PDF report.	
	<i>disable</i>	Disable PDF report.	
report-source	Report log source.	option	-
	Option	Description	
	<i>forward-traffic</i>	Report includes forward traffic logs.	
	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.	
	<i>local-deny-traffic</i>	Report includes local deny traffic logs.	
top-n	Number of items to populate (1000 - 20000).	integer	Minimum value: 1000 Maximum value: 20000
web-browsing-threshold	Web browsing time calculation threshold (3 - 15 min).	integer	Minimum value: 3 Maximum value: 15

config report style



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report style configuration.

```
config report style
  Description: Report style configuration.
  edit <name>
    set align [left|center|...]
    set bg-color {string}
    set border-bottom {user}
    set border-left {user}
    set border-right {user}
    set border-top {user}
    set column-gap {string}
    set column-span [none|all]
    set fg-color {string}
    set font-family [Verdana|Arial|...]
    set font-size {string}
    set font-style [normal|italic]
    set font-weight [normal|bold]
    set height {string}
    set line-height {string}
    set margin-bottom {string}
    set margin-left {string}
    set margin-right {string}
    set margin-top {string}
    set options {option1}, {option2}, ...
```

```

        set padding-bottom {string}
        set padding-left {string}
        set padding-right {string}
        set padding-top {string}
        set width {string}
    next
end

```

config report style

Parameter	Description	Type	Size
align	Alignment.	option	-
	Option	Description	
	left	Align left.	
	center	Align center.	
	right	Align right.	
	justify	Align justify.	
bg-color	Background color.	string	Maximum length: 15
border-bottom	Border bottom.	user	Not Specified
border-left	Border left.	user	Not Specified
border-right	Border right.	user	Not Specified
border-top	Border top.	user	Not Specified
column-gap	Column gap.	string	Maximum length: 15
column-span	Column span.	option	-
	Option	Description	
	none	Does not span.	
	all	Span across all columns.	
fg-color	Foreground color.	string	Maximum length: 15
font-family	Font family.	option	-

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>Verdana</i></td><td>Verdana.</td></tr><tr><td><i>Arial</i></td><td>Arial.</td></tr><tr><td><i>Helvetica</i></td><td>Helvetica.</td></tr><tr><td><i>Courier</i></td><td>Courier.</td></tr><tr><td><i>Times</i></td><td>Times Roman.</td></tr></table>	Option	Description	<i>Verdana</i>	Verdana.	<i>Arial</i>	Arial.	<i>Helvetica</i>	Helvetica.	<i>Courier</i>	Courier.	<i>Times</i>	Times Roman.		
	Option	Description													
	<i>Verdana</i>	Verdana.													
	<i>Arial</i>	Arial.													
	<i>Helvetica</i>	Helvetica.													
	<i>Courier</i>	Courier.													
	<i>Times</i>	Times Roman.													
font-size	Font size.	string	Maximum length: 15												
font-style	Font style.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal.</td></tr><tr><td><i>italic</i></td><td>Italic.</td></tr></table>	Option	Description	<i>normal</i>	Normal.	<i>italic</i>	Italic.								
	Option	Description													
	<i>normal</i>	Normal.													
<i>italic</i>	Italic.														
font-weight	Font weight.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal.</td></tr><tr><td><i>bold</i></td><td>Bold.</td></tr></table>	Option	Description	<i>normal</i>	Normal.	<i>bold</i>	Bold.								
	Option	Description													
	<i>normal</i>	Normal.													
<i>bold</i>	Bold.														
height	Height.	string	Maximum length: 15												
line-height	Text line height.	string	Maximum length: 15												
margin-bottom	Margin bottom.	string	Maximum length: 15												
margin-left	Margin left.	string	Maximum length: 15												
margin-right	Margin right.	string	Maximum length: 15												
margin-top	Margin top.	string	Maximum length: 15												
name	Report style name.	string	Maximum length: 71												
options	Report style options.	option	-												

Parameter	Description	Type	Size

	Option	Description		
	<i>font</i>	Font.		
	<i>text</i>	Text.		
	<i>color</i>	Color.		
	<i>align</i>	Align.		
	<i>size</i>	Size.		
	<i>margin</i>	Margin.		
	<i>border</i>	Border.		
	<i>padding</i>	Padding.		
	<i>column</i>	Column.		

padding-bottom	Padding bottom.	string	Maximum length: 15
padding-left	Padding left.	string	Maximum length: 15
padding-right	Padding right.	string	Maximum length: 15
padding-top	Padding top.	string	Maximum length: 15
width	Width.	string	Maximum length: 15

config report theme



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report themes configuration

config report theme

Description: Report themes configuration

edit <name>

```
set bullet-list-style {string}
set column-count [1|2|...]
set default-html-style {string}
set default-pdf-style {string}
set graph-chart-style {string}
set heading1-style {string}
set heading2-style {string}
set heading3-style {string}
set heading4-style {string}
set hline-style {string}
set image-style {string}
set normal-text-style {string}
set numbered-list-style {string}
set page-footer-style {string}
set page-header-style {string}
set page-orient [portrait|landscape]
set page-style {string}
set report-subtitle-style {string}
set report-title-style {string}
set table-chart-caption-style {string}
```



```

set table-chart-even-row-style {string}
set table-chart-head-style {string}
set table-chart-odd-row-style {string}
set table-chart-style {string}
set toc-heading1-style {string}
set toc-heading2-style {string}
set toc-heading3-style {string}
set toc-heading4-style {string}
set toc-title-style {string}
next
end

```

config report theme

Parameter	Description	Type	Size								
bullet-list-style	Bullet list style.	string	Maximum length: 71								
column-count	Report page column count.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>One Column.</td></tr><tr><td>2</td><td>Two Columns.</td></tr><tr><td>3</td><td>Three Columns.</td></tr></table>	Option	Description	1	One Column.	2	Two Columns.	3	Three Columns.		
	Option	Description									
	1	One Column.									
	2	Two Columns.									
3	Three Columns.										
default-html-style	Default HTML report style.	string	Maximum length: 71								
default-pdf-style	Default PDF report style.	string	Maximum length: 71								
graph-chart-style	Graph chart style.	string	Maximum length: 71								
heading1-style	Report heading style.	string	Maximum length: 71								
heading2-style	Report heading style.	string	Maximum length: 71								
heading3-style	Report heading style.	string	Maximum length: 71								
heading4-style	Report heading style.	string	Maximum length: 71								
hline-style	Horizontal line style.	string	Maximum length: 71								
image-style	Image style.	string	Maximum length: 71								

Parameter	Description	Type	Size						
name	Report theme name.	string	Maximum length: 35						
normal-text-style	Normal text style.	string	Maximum length: 71						
numbered-list-style	Numbered list style.	string	Maximum length: 71						
page-footer-style	Report page footer style.	string	Maximum length: 71						
page-header-style	Report page header style.	string	Maximum length: 71						
page-orient	Report page orientation.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>portrait</i></td><td>Portrait Orientation.</td></tr><tr><td><i>landscape</i></td><td>Landscape Orientation.</td></tr></table>			Option	Description	<i>portrait</i>	Portrait Orientation.	<i>landscape</i>	Landscape Orientation.
	Option	Description							
	<i>portrait</i>	Portrait Orientation.							
<i>landscape</i>	Landscape Orientation.								
page-style	Report page style.	string	Maximum length: 71						
report-subtitle-style	Report subtitle style.	string	Maximum length: 71						
report-title-style	Report title style.	string	Maximum length: 71						
table-chart-caption-style	Table chart caption style.	string	Maximum length: 71						
table-chart-even-row-style	Table chart even row style.	string	Maximum length: 71						
table-chart-head-style	Table chart head row style.	string	Maximum length: 71						
table-chart-odd-row-style	Table chart odd row style.	string	Maximum length: 71						
table-chart-style	Table chart style.	string	Maximum length: 71						
toc-heading1-style	Table of contents heading style.	string	Maximum length: 71						
toc-heading2-style	Table of contents heading style.	string	Maximum length: 71						

Parameter	Description	Type	Size
toc-heading3-style	Table of contents heading style.	string	Maximum length: 71
toc-heading4-style	Table of contents heading style.	string	Maximum length: 71
toc-title-style	Table of contents title style.	string	Maximum length: 71

router

This section includes syntax for the following commands:

- [config router access-list on page 612](#)
- [config router access-list6 on page 614](#)
- [config router aspath-list on page 615](#)
- [config router auth-path on page 616](#)
- [config router bfd on page 616](#)
- [config router bfd6 on page 617](#)
- [config router bgp on page 617](#)
- [config router community-list on page 656](#)
- [config router isis on page 657](#)
- [config router key-chain on page 670](#)
- [config router multicast-flow on page 682](#)
- [config router multicast on page 671](#)
- [config router multicast6 on page 680](#)
- [config router ospf on page 683](#)
- [config router ospf6 on page 698](#)
- [config router policy on page 711](#)
- [config router policy6 on page 714](#)
- [config router prefix-list on page 715](#)
- [config router prefix-list6 on page 717](#)
- [config router rip on page 718](#)
- [config router ripng on page 725](#)
- [config router route-map on page 731](#)
- [config router setting on page 736](#)
- [config router static on page 737](#)
- [config router static6 on page 740](#)

config router access-list

Configure access lists.

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

```

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

```

config router access-list

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

config rule

Parameter	Description	Type	Size
action	Permit or deny this IP address and netmask prefix.	option	-
	Option	Description	
	<i>permit</i>	Permit or allow this IP address and netmask prefix.	
	<i>deny</i>	Deny this IP address and netmask prefix.	
exact-match	Enable/disable exact match.	option	-
	Option	Description	
	<i>enable</i>	Enable exact match.	
	<i>disable</i>	Disable exact match.	
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295

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

config router access-list6

Configure IPv6 access lists.

```

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

```

config router access-list6

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

config rule

Parameter	Description	Type	Size
action	Permit or deny this IP address and netmask prefix.	option	-
	Option	Description	
	<i>permit</i>	Permit or allow this IP address and netmask prefix.	
	<i>deny</i>	Deny this IP address and netmask prefix.	
exact-match	Enable/disable exact prefix match.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable exact match.	
	<i>disable</i>	Disable exact match.	
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified

config router aspath-list

Configure Autonomous System (AS) path lists.

```

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

```

config router aspath-list

Parameter	Description	Type	Size
name	AS path list name.	string	Maximum length: 35

config rule

Parameter	Description	Type	Size						
action	Permit or deny route-based operations, based on the route's AS_PATH attribute.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Deny route-based operations.</td></tr><tr><td><i>permit</i></td><td>Permit route-based operations.</td></tr></table>	Option	Description	<i>deny</i>	Deny route-based operations.	<i>permit</i>	Permit route-based operations.		
Option	Description								
<i>deny</i>	Deny route-based operations.								
<i>permit</i>	Permit route-based operations.								
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295						
regexp	Regular-expression to match the Border Gateway Protocol (BGP) AS paths.	string	Maximum length: 63						

config router auth-path

Configure authentication based routing.

```
config router auth-path
  Description: Configure authentication based routing.
  edit <name>
    set device {string}
    set gateway {ipv4-address}
  next
end
```

config router auth-path

Parameter	Description	Type	Size
device	Outgoing interface.	string	Maximum length: 35
gateway	Gateway IP address.	ipv4-address	Not Specified
name	Name of the entry.	string	Maximum length: 15

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
ip	IPv4 address of the BFD neighbor.	ipv4-address	Not Specified

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
ip6-address	IPv6 address of the BFD neighbor.	ipv6-address	Not Specified

config router bgp

Configure BGP.

```
config router bgp
  Description: Configure BGP.
  set additional-path [enable|disable]
  set additional-path-select {integer}
```

```

set additional-path-select6 {integer}
set additional-path6 [enable|disable]
config admin-distance
    Description: Administrative distance modifications.
    edit <id>
        set distance {integer}
        set neighbour-prefix {ipv4-classnet}
        set route-list {string}
    next
end
config aggregate-address
    Description: BGP aggregate address table.
    edit <id>
        set as-set [enable|disable]
        set prefix {ipv4-classnet-any}
        set summary-only [enable|disable]
    next
end
config aggregate-address6
    Description: BGP IPv6 aggregate address table.
    edit <id>
        set as-set [enable|disable]
        set prefix6 {ipv6-prefix}
        set summary-only [enable|disable]
    next
end
set always-compare-med [enable|disable]
set as {integer}
set bestpath-as-path-ignore [enable|disable]
set bestpath-cmp-confed-aspath [enable|disable]
set bestpath-cmp-routerid [enable|disable]
set bestpath-med-confed [enable|disable]
set bestpath-med-missing-as-worst [enable|disable]
set client-to-client-reflection [enable|disable]
set cluster-id {ipv4-address-any}
set confederation-identifier {integer}
set confederation-peers <peer1>, <peer2>, ...
set dampening [enable|disable]
set dampening-max-suppress-time {integer}
set dampening-reachability-half-life {integer}
set dampening-reuse {integer}
set dampening-route-map {string}
set dampening-suppress {integer}
set dampening-unreachability-half-life {integer}
set default-local-preference {integer}
set deterministic-med [enable|disable]
set distance-external {integer}
set distance-internal {integer}
set distance-local {integer}
set ebgp-multipath [enable|disable]
set enforce-first-as [enable|disable]
set fast-external-failover [enable|disable]
set graceful-end-on-timer [enable|disable]
set graceful-restart [enable|disable]
set graceful-restart-time {integer}
set graceful-stalepath-time {integer}

```

```

set graceful-update-delay {integer}
set holdtime-timer {integer}
set ibgp-multipath [enable|disable]
set ignore-optional-capability [enable|disable]
set keepalive-timer {integer}
set log-neighbour-changes [enable|disable]
config neighbor
    Description: BGP neighbor table.
    edit <ip>
        set activate [enable|disable]
        set activate6 [enable|disable]
        set additional-path [send|receive|...]
        set additional-path6 [send|receive|...]
        set adv-additional-path {integer}
        set adv-additional-path6 {integer}
        set advertisement-interval {integer}
        set allowas-in {integer}
        set allowas-in-enable [enable|disable]
        set allowas-in-enable6 [enable|disable]
        set allowas-in6 {integer}
        set as-override [enable|disable]
        set as-override6 [enable|disable]
        set attribute-unchanged {option1}, {option2}, ...
        set attribute-unchanged6 {option1}, {option2}, ...
        set bfd [enable|disable]
        set capability-default-originate [enable|disable]
        set capability-default-originate6 [enable|disable]
        set capability-dynamic [enable|disable]
        set capability-graceful-restart [enable|disable]
        set capability-graceful-restart6 [enable|disable]
        set capability-orf [none|receive|...]
        set capability-orf6 [none|receive|...]
        set capability-route-refresh [enable|disable]
    config conditional-advertise
        Description: Conditional advertisement.
        edit <advertise-routemap>
            set condition-routemap {string}
            set condition-type [exist|non-exist]
        next
    end
    set connect-timer {integer}
    set default-originate-routemap {string}
    set default-originate-routemap6 {string}
    set description {string}
    set distribute-list-in {string}
    set distribute-list-in6 {string}
    set distribute-list-out {string}
    set distribute-list-out6 {string}
    set dont-capability-negotiate [enable|disable]
    set ebgp-enforce-multihop [enable|disable]
    set ebgp-multihop-ttl {integer}
    set filter-list-in {string}
    set filter-list-in6 {string}
    set filter-list-out {string}
    set filter-list-out6 {string}
    set holdtime-timer {integer}

```

```

    set interface {string}
    set keep-alive-timer {integer}
    set link-down-failover [enable|disable]
    set local-as {integer}
    set local-as-no-prepend [enable|disable]
    set local-as-replace-as [enable|disable]
    set maximum-prefix {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 maximum-prefix6 {integer}
    set next-hop-self [enable|disable]
    set next-hop-self6 [enable|disable]
    set override-capability [enable|disable]
    set passive [enable|disable]
    set password {password}
    set prefix-list-in {string}
    set prefix-list-in6 {string}
    set prefix-list-out {string}
    set prefix-list-out6 {string}
    set remote-as {integer}
    set remove-private-as [enable|disable]
    set remove-private-as6 [enable|disable]
    set restart-time {integer}
    set retain-stale-time {integer}
    set route-map-in {string}
    set route-map-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 route-reflector-client [enable|disable]
    set route-reflector-client6 [enable|disable]
    set route-server-client [enable|disable]
    set route-server-client6 [enable|disable]
    set send-community [standard|extended|...]
    set send-community6 [standard|extended|...]
    set shutdown [enable|disable]
    set soft-reconfiguration [enable|disable]
    set soft-reconfiguration6 [enable|disable]
    set stale-route [enable|disable]
    set strict-capability-match [enable|disable]
    set unsuppress-map {string}
    set unsuppress-map6 {string}
    set update-source {string}
    set weight {integer}
next
end
config neighbor-group
    Description: BGP neighbor group table.
    edit <name>
        set activate [enable|disable]
        set activate6 [enable|disable]
        set additional-path [send|receive|...]
        set additional-path6 [send|receive|...]

```

```
set adv-additional-path {integer}
set adv-additional-path6 {integer}
set advertisement-interval {integer}
set allowas-in {integer}
set allowas-in-enable [enable|disable]
set allowas-in-enable6 [enable|disable]
set allowas-in6 {integer}
set as-override [enable|disable]
set as-override6 [enable|disable]
set attribute-unchanged {option1}, {option2}, ...
set attribute-unchanged6 {option1}, {option2}, ...
set bfd [enable|disable]
set capability-default-originate [enable|disable]
set capability-default-originate6 [enable|disable]
set capability-dynamic [enable|disable]
set capability-graceful-restart [enable|disable]
set capability-graceful-restart6 [enable|disable]
set capability-orf [none|receive|...]
set capability-orf6 [none|receive|...]
set capability-route-refresh [enable|disable]
set connect-timer {integer}
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set holdtime-timer {integer}
set interface {string}
set keep-alive-timer {integer}
set link-down-failover [enable|disable]
set local-as {integer}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set maximum-prefix {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 maximum-prefix6 {integer}
set next-hop-self [enable|disable]
set next-hop-self6 [enable|disable]
set override-capability [enable|disable]
set passive [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 remove-private-as [enable|disable]
        set remove-private-as6 [enable|disable]
        set restart-time {integer}
        set retain-stale-time {integer}
        set route-map-in {string}
        set route-map-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 route-reflector-client [enable|disable]
        set route-reflector-client6 [enable|disable]
        set route-server-client [enable|disable]
        set route-server-client6 [enable|disable]
        set send-community [standard|extended|...]
        set send-community6 [standard|extended|...]
        set shutdown [enable|disable]
        set soft-reconfiguration [enable|disable]
        set soft-reconfiguration6 [enable|disable]
        set stale-route [enable|disable]
        set strict-capability-match [enable|disable]
        set unsuppress-map {string}
        set unsuppress-map6 {string}
        set update-source {string}
        set weight {integer}
    next
end
config neighbor-range
    Description: BGP neighbor range table.
    edit <id>
        set max-neighbor-num {integer}
        set neighbor-group {string}
        set prefix {ipv4-classnet}
    next
end
config neighbor-range6
    Description: BGP IPv6 neighbor range table.
    edit <id>
        set max-neighbor-num {integer}
        set neighbor-group {string}
        set prefix6 {ipv6-network}
    next
end
config network
    Description: BGP network table.
    edit <id>
        set backdoor [enable|disable]
        set prefix {ipv4-classnet}
        set route-map {string}
    next
end
set network-import-check [enable|disable]
config network6
    Description: BGP IPv6 network table.
    edit <id>

```

```

        set backdoor [enable|disable]
        set prefix6 {ipv6-network}
        set route-map {string}
    next
end
config redistribute
    Description: BGP IPv4 redistribute table. Read-only.
    edit <name>
        set route-map {string}
        set status [enable|disable]
    next
end
config redistribute6
    Description: BGP IPv6 redistribute table. Read-only.
    edit <name>
        set route-map {string}
        set status [enable|disable]
    next
end
set router-id {ipv4-address-any}
set scan-time {integer}
set synchronization [enable|disable]
end

```

config router bgp

Parameter	Description	Type	Size						
additional-path	Enable/disable selection of BGP IPv4 additional paths.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
additional-path-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						
additional-path6	Enable/disable selection of BGP IPv6 additional paths.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
always-compare-med	Enable/disable always compare MED.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
as	Router AS number, valid from 1 to 4294967295, 0 to disable BGP.	integer	Minimum value: 0 Maximum value: 4294967295
bestpath-as-path-ignore	Enable/disable ignore AS path.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
bestpath-cmp-confed-aspath	Enable/disable compare federation AS path length.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
bestpath-cmp-routerid	Enable/disable compare router ID for identical EBGp paths.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
bestpath-med-confed	Enable/disable compare MED among confederation paths.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
bestpath-med-missing-as-worst	Enable/disable treat missing MED as least preferred.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
client-to-client-reflection	Enable/disable client-to-client route reflection.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	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	Enable/disable route-flap dampening.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
dampening-max-suppress-time	Maximum minutes a route can be suppressed.	integer	Minimum value: 1 Maximum value: 255

Parameter	Description	Type	Size
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
dampening-route-map	Criteria for dampening.	string	Maximum length: 35
dampening-suppress	Threshold to suppress routes.	integer	Minimum value: 1 Maximum value: 20000
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
deterministic-med	Enable/disable enforce deterministic comparison of MED.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
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

Parameter	Description	Type	Size						
distance-local	Distance for routes local to the AS.	integer	Minimum value: 1 Maximum value: 255						
ebgp-multipath	Enable/disable EBGp multi-path.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
enforce-first-as	Enable/disable enforce first AS for EBGp routes.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
fast-external-failover	Enable/disable reset peer BGP session if link goes down.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
graceful-end-on-timer	Enable/disable to exit graceful restart on timer only.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
graceful-restart	Enable/disable BGP graceful restart capabilities.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
graceful-restart-time	Time needed for neighbors to restart (sec).	integer	Minimum value: 1 Maximum value: 3600						

Parameter	Description	Type	Size						
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						
holdtime-timer	Number of seconds to mark peer as dead.	integer	Minimum value: 3 Maximum value: 65535						
ibgp-multipath	Enable/disable IBGP multi-path.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
ignore-optional-capability	Don't send unknown optional capability notification message	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
keepalive-timer	Frequency to send keep alive requests.	integer	Minimum value: 0 Maximum value: 65535						
log-neighbour-changes	Enable logging of BGP neighbour's changes	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
network-import-check	Enable/disable ensure BGP network route exists in IGP.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
router-id	Router ID.	ipv4-address-any	Not Specified
scan-time	Background scanner interval (sec), 0 to disable it.	integer	Minimum value: 5 Maximum value: 60
synchronization	Enable/disable only advertise routes from iBGP if routes present in an IGP.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config admin-distance

Parameter	Description	Type	Size
distance	Administrative distance to apply (1 - 255).	integer	Minimum value: 1 Maximum value: 255
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
neighbour-prefix	Neighbor address prefix.	ipv4-classnet	Not Specified
route-list	Access list of routes to apply new distance to.	string	Maximum length: 35

config aggregate-address

Parameter	Description	Type	Size
as-set	Enable/disable generate AS set path information.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix	Aggregate prefix.	ipv4-classnet-any	Not Specified
summary-only	Enable/disable filter more specific routes from updates.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config aggregate-address6

Parameter	Description	Type	Size
as-set	Enable/disable generate AS set path information.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	Aggregate IPv6 prefix.	ipv6-prefix	Not Specified
summary-only	Enable/disable filter more specific routes from updates.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config neighbor

Parameter	Description	Type	Size
activate	Enable/disable address family IPv4 for this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
activate6	Enable/disable address family IPv6 for this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
additional-path	Enable/disable IPv4 additional-path capability.	option	-
	Option	Description	
	<i>send</i>	Enable sending additional paths.	
	<i>receive</i>	Enable receiving additional paths.	
	<i>both</i>	Enable sending and receiving additional paths.	
	<i>disable</i>	Disable additional paths.	
additional-path6	Enable/disable IPv6 additional-path capability.	option	-
	Option	Description	
	<i>send</i>	Enable sending additional paths.	
	<i>receive</i>	Enable receiving additional paths.	
	<i>both</i>	Enable sending and receiving additional paths.	
	<i>disable</i>	Disable additional paths.	
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 4
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 4

Parameter	Description	Type	Size						
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 1 Maximum value: 600						
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10						
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10						
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size								
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.		
Option	Description										
<i>as-path</i>	AS path.										
<i>med</i>	MED.										
<i>next-hop</i>	Next hop.										
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.		
Option	Description										
<i>as-path</i>	AS path.										
<i>med</i>	MED.										
<i>next-hop</i>	Next hop.										
bfd	Enable/disable BFD for this neighbor.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-
	Option	Description	
	<i>none</i>	None.	
	<i>receive</i>	Receive ORF lists.	
	<i>send</i>	Send ORF list.	
	<i>both</i>	Send and receive ORF lists.	
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-
	Option	Description	
	<i>none</i>	None.	
	<i>receive</i>	Receive ORF lists.	
	<i>send</i>	Send ORF list.	
	<i>both</i>	Send and receive ORF lists.	
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535						
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						
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size						
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						
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535						
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15						
ip	IP/IPv6 address of neighbor.	string	Maximum length: 45						
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535						
link-down-failover	Enable/disable failover upon link down.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295						
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295
maximum-prefix-threshold	Maximum IPv4 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value (1 - 100 percent).	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	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size						
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295						
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
override-capability	Enable/disable override result of capability negotiation.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
passive	Enable/disable sending of open messages to this neighbor.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
password	Password used in MD5 authentication.	password	Not Specified						
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35						
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						

Parameter	Description	Type	Size
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
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
restart-time	Graceful restart delay time (sec, 0 = global default).	integer	Minimum value: 0 Maximum value: 3600
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35
route-map-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

Parameter	Description	Type	Size
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
route-server-client	Enable/disable IPv4 AS route server client.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
route-server-client6	Enable/disable IPv6 AS route server client.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
send-community	IPv4 Send community attribute to neighbor.	option	-
	Option	Description	
	<i>standard</i>	Standard.	
	<i>extended</i>	Extended.	
	<i>both</i>	Both.	
	<i>disable</i>	Disable	
send-community6	IPv6 Send community attribute to neighbor.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable		
	Option	Description											
	<i>standard</i>	Standard.											
	<i>extended</i>	Extended.											
	<i>both</i>	Both.											
<i>disable</i>	Disable												
shutdown	Enable/disable shutdown this neighbor.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
stale-route	Enable/disable stale route after neighbor down.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
strict-capability-match	Enable/disable strict capability matching.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												

Parameter	Description	Type	Size
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

config conditional-advertise

Parameter	Description	Type	Size
advertise-routemap	Name of advertising route map.	string	Maximum length: 35
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
activate	Enable/disable address family IPv4 for this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
activate6	Enable/disable address family IPv6 for this neighbor.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
additional-path	Enable/disable IPv4 additional-path capability.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.		
	Option	Description											
	<i>send</i>	Enable sending additional paths.											
	<i>receive</i>	Enable receiving additional paths.											
	<i>both</i>	Enable sending and receiving additional paths.											
<i>disable</i>	Disable additional paths.												
additional-path6	Enable/disable IPv6 additional-path capability.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.		
	Option	Description											
	<i>send</i>	Enable sending additional paths.											
	<i>receive</i>	Enable receiving additional paths.											
	<i>both</i>	Enable sending and receiving additional paths.											
<i>disable</i>	Disable additional paths.												
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 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										
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 1 Maximum value: 600										
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10										
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-										

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-
	Option	Description	
	<i>as-path</i>	AS path.	
	<i>med</i>	MED.	
	<i>next-hop</i>	Next hop.	
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>as-path</i>	AS path.	
	<i>med</i>	MED.	
	<i>next-hop</i>	Next hop.	
bfd	Enable/disable BFD for this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size										
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
Option	Description												
<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.												
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.		
Option	Description												
<i>none</i>	None.												
<i>receive</i>	Receive ORF lists.												
<i>send</i>	Send ORF list.												
<i>both</i>	Send and receive ORF lists.												
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.		
Option	Description												
<i>none</i>	None.												
<i>receive</i>	Receive ORF lists.												
<i>send</i>	Send ORF list.												
<i>both</i>	Send and receive ORF lists.												
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
Option	Description												
<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.												
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535										
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										

Parameter	Description	Type	Size						
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						
dont-capability-negotiate	Don't negotiate capabilities with this neighbor	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255						
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						

Parameter	Description	Type	Size
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535
link-down-failover	Enable/disable failover upon link down.	option	-
	Option		Description
	<i>enable</i>		Enable setting.
	<i>disable</i>		Disable setting.
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
	<i>enable</i>		Enable setting.
	<i>disable</i>		Disable setting.
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-
	Option		Description
	<i>enable</i>		Enable setting.
	<i>disable</i>		Disable setting.
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295

Parameter	Description	Type	Size						
maximum-prefix-threshold	Maximum IPv4 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100						
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value (1 - 100 percent).	integer	Minimum value: 1 Maximum value: 100						
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295						
name	Neighbor group name.	string	Maximum length: 45						
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
override-capability	Enable/disable override result of capability negotiation.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
passive	Enable/disable sending of open messages to this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
restart-time	Graceful restart delay time (sec, 0 = global default).	integer	Minimum value: 0 Maximum value: 3600						
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535						
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35						
route-map-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						
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
route-server-client	Enable/disable IPv4 AS route server client.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
route-server-client6	Enable/disable IPv6 AS route server client.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
send-community	IPv4 Send community attribute to neighbor.	option	-
	Option	Description	
	<i>standard</i>	Standard.	
	<i>extended</i>	Extended.	
	<i>both</i>	Both.	
	<i>disable</i>	Disable	
send-community6	IPv6 Send community attribute to neighbor.	option	-
	Option	Description	
	<i>standard</i>	Standard.	
	<i>extended</i>	Extended.	
	<i>both</i>	Both.	
	<i>disable</i>	Disable	
shutdown	Enable/disable shutdown this neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size						
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
stale-route	Enable/disable stale route after neighbor down.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
strict-capability-match	Enable/disable strict capability matching.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35						
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35						
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15						
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535						

config neighbor-range

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

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
prefix	Neighbor range prefix.	ipv4-classnet	Not Specified

config neighbor-range6

Parameter	Description	Type	Size
id	IPv6 neighbor range ID.	integer	Minimum value: 0 Maximum value: 4294967295
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000
neighbor-group	Neighbor group name.	string	Maximum length: 63
prefix6	IPv6 prefix.	ipv6-network	Not Specified

config network

Parameter	Description	Type	Size						
backdoor	Enable/disable route as backdoor.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
	<i>disable</i>	Disable setting.							
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295						
prefix	Network prefix.	ipv4-classnet	Not Specified						
route-map	Route map to modify generated route.	string	Maximum length: 35						

config network6

Parameter	Description	Type	Size
backdoor	Enable/disable route as backdoor.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	Network IPv6 prefix.	ipv6-network	Not Specified
route-map	Route map to modify generated route.	string	Maximum length: 35

config redistribute

Parameter	Description	Type	Size
name	Distribute list entry name.	string	Maximum length: 35
route-map	Route map name.	string	Maximum length: 35
status	Status	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config redistribute6

Parameter	Description	Type	Size
name	Distribute list entry name.	string	Maximum length: 35
route-map	Route map name.	string	Maximum length: 35
status	Status	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config router community-list

Configure community lists.

```

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

```

config router community-list

Parameter	Description	Type	Size
name	Community list name.	string	Maximum length: 35
type	Community list type (standard or expanded).	option	-
	Option	Description	
	<i>standard</i>	Standard community list type.	
	<i>expanded</i>	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	-

Parameter	Description	Type	Size
	Option	Description	
	<i>deny</i>	Deny route-based operations.	
	<i>permit</i>	Permit or allow route-based operations.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
match	Community specifications for matching a reserved community.	string	Maximum length: 255
regex	Ordered list of COMMUNITY attributes as a regular expression.	string	Maximum length: 255

config router isis

Configure IS-IS.

```
config router isis
  Description: Configure IS-IS.
  set adjacency-check [enable|disable]
  set adjacency-check6 [enable|disable]
  set adv-passive-only [enable|disable]
  set adv-passive-only6 [enable|disable]
  set auth-keychain-l1 {string}
  set auth-keychain-l2 {string}
  set auth-mode-l1 [password|md5]
  set auth-mode-l2 [password|md5]
  set auth-password-l1 {password}
  set auth-password-l2 {password}
  set auth-sendonly-l1 [enable|disable]
  set auth-sendonly-l2 [enable|disable]
  set default-originate [enable|disable]
  set default-originate6 [enable|disable]
  set dynamic-hostname [enable|disable]
  set ignore-lsp-errors [enable|disable]
  set is-type [level-1-2|level-1|...]
  config isis-interface
    Description: IS-IS interface configuration.
    edit <name>
      set auth-keychain-l1 {string}
      set auth-keychain-l2 {string}
      set auth-mode-l1 [md5|password]
      set auth-mode-l2 [md5|password]
      set auth-password-l1 {password}
      set auth-password-l2 {password}
      set auth-send-only-l1 [enable|disable]
      set auth-send-only-l2 [enable|disable]
```

```

        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 mesh-group [enable|disable]
        set mesh-group-id {integer}
        set metric-l1 {integer}
        set metric-l2 {integer}
        set network-type [broadcast|point-to-point|...]
        set priority-l1 {integer}
        set priority-l2 {integer}
        set status [enable|disable]
        set status6 [enable|disable]
        set wide-metric-l1 {integer}
        set wide-metric-l2 {integer}
    next
end
config isis-net
    Description: IS-IS net configuration.
    edit <id>
        set net {user}
    next
end
set lsp-gen-interval-l1 {integer}
set lsp-gen-interval-l2 {integer}
set lsp-refresh-interval {integer}
set max-lsp-lifetime {integer}
set metric-style [narrow|wide|...]
set overload-bit [enable|disable]
set overload-bit-on-startup {integer}
set overload-bit-suppress {option1}, {option2}, ...
config redistribute
    Description: IS-IS redistribute protocols. Read-only.
    edit <protocol>
        set level [level-1-2|level-1|...]
        set metric {integer}
        set metric-type [external|internal]
        set routemap {string}
        set status [enable|disable]
    next
end
set redistribute-l1 [enable|disable]
set redistribute-l1-list {string}
set redistribute-l2 [enable|disable]
set redistribute-l2-list {string}
config redistribute6
    Description: IS-IS IPv6 redistribution for routing protocols. Read-only.
    edit <protocol>
        set level [level-1-2|level-1|...]
        set metric {integer}

```

```

        set metric-type [external|internal]
        set routemap {string}
        set status [enable|disable]
    next
end
set redistribute6-l1 [enable|disable]
set redistribute6-l1-list {string}
set redistribute6-l2 [enable|disable]
set redistribute6-l2-list {string}
set spf-interval-exp-l1 {user}
set spf-interval-exp-l2 {user}
config summary-address
    Description: IS-IS summary addresses.
    edit <id>
        set level [level-1-2|level-1|...]
        set prefix {ipv4-classnet-any}
    next
end
config summary-address6
    Description: IS-IS IPv6 summary address.
    edit <id>
        set level [level-1-2|level-1|...]
        set prefix6 {ipv6-prefix}
    next
end
end

```

config router isis

Parameter	Description	Type	Size
adjacency-check	Enable/disable adjacency check.	option	-
	Option	Description	
	<i>enable</i>	Enable adjacency check.	
	<i>disable</i>	Disable adjacency check.	
adjacency-check6	Enable/disable IPv6 adjacency check.	option	-
	Option	Description	
	<i>enable</i>	Enable IPv6 adjacency check.	
	<i>disable</i>	Disable IPv6 adjacency check.	
adv-passive-only	Enable/disable IS-IS advertisement of passive interfaces only.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Advertise passive interfaces only.	
	<i>disable</i>	Advertise all IS-IS enabled interfaces.	
adv-passive-only6	Enable/disable IPv6 IS-IS advertisement of passive interfaces only.	option	-
	Option	Description	
	<i>enable</i>	Advertise passive interfaces only.	
	<i>disable</i>	Advertise all IS-IS enabled interfaces.	
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35
auth-mode-l1	Level 1 authentication mode.	option	-
	Option	Description	
	<i>password</i>	Password.	
	<i>md5</i>	MD5.	
auth-mode-l2	Level 2 authentication mode.	option	-
	Option	Description	
	<i>password</i>	Password.	
	<i>md5</i>	MD5.	
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified
auth-sendonly-l1	Enable/disable level 1 authentication send-only.	option	-
	Option	Description	
	<i>enable</i>	Enable level 1 authentication send-only.	
	<i>disable</i>	Disable level 1 authentication send-only.	

Parameter	Description	Type	Size								
auth-sendonly-l2	Enable/disable level 2 authentication send-only.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable level 2 authentication send-only.</td></tr><tr><td><i>disable</i></td><td>Disable level 2 authentication send-only.</td></tr></table>	Option	Description	<i>enable</i>	Enable level 2 authentication send-only.	<i>disable</i>	Disable level 2 authentication send-only.				
Option	Description										
<i>enable</i>	Enable level 2 authentication send-only.										
<i>disable</i>	Disable level 2 authentication send-only.										
default-originate	Enable/disable distribution of default route information.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distribution of default route information.</td></tr><tr><td><i>disable</i></td><td>Disable distribution of default route information.</td></tr></table>	Option	Description	<i>enable</i>	Enable distribution of default route information.	<i>disable</i>	Disable distribution of default route information.				
Option	Description										
<i>enable</i>	Enable distribution of default route information.										
<i>disable</i>	Disable distribution of default route information.										
default-originate6	Enable/disable distribution of default IPv6 route information.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distribution of default IPv6 route information.</td></tr><tr><td><i>disable</i></td><td>Disable distribution of default IPv6 route information.</td></tr></table>	Option	Description	<i>enable</i>	Enable distribution of default IPv6 route information.	<i>disable</i>	Disable distribution of default IPv6 route information.				
Option	Description										
<i>enable</i>	Enable distribution of default IPv6 route information.										
<i>disable</i>	Disable distribution of default IPv6 route information.										
dynamic-hostname	Enable/disable dynamic hostname.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic hostname.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic hostname.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic hostname.	<i>disable</i>	Disable dynamic hostname.				
Option	Description										
<i>enable</i>	Enable dynamic hostname.										
<i>disable</i>	Disable dynamic hostname.										
ignore-lsp-errors	Enable/disable ignoring of LSP errors with bad checksums.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring of LSP errors with bad checksums.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring of LSP errors with bad checksums.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring of LSP errors with bad checksums.	<i>disable</i>	Disable ignoring of LSP errors with bad checksums.				
Option	Description										
<i>enable</i>	Enable ignoring of LSP errors with bad checksums.										
<i>disable</i>	Disable ignoring of LSP errors with bad checksums.										
is-type	IS type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>level-1-2</i></td><td>Level 1 and 2.</td></tr><tr><td><i>level-1</i></td><td>Level 1 only.</td></tr><tr><td><i>level-2-only</i></td><td>Level 2 only.</td></tr></table>	Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1 only.	<i>level-2-only</i>	Level 2 only.		
Option	Description										
<i>level-1-2</i>	Level 1 and 2.										
<i>level-1</i>	Level 1 only.										
<i>level-2-only</i>	Level 2 only.										

Parameter	Description	Type	Size
lsp-gen-interval-l1	Minimum interval for level 1 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120
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
metric-style	Use old-style (ISO 10589) or new-style packet formats	option	-

Option	Description
<i>narrow</i>	Use old style of TLVs with narrow metric.
<i>wide</i>	Use new style of TLVs to carry wider metric.
<i>transition</i>	Send and accept both styles of TLVs during transition.
<i>narrow-transition</i>	Narrow and accept both styles of TLVs during transition.
<i>narrow-transition-l1</i>	Narrow-transition level-1 only.
<i>narrow-transition-l2</i>	Narrow-transition level-2 only.
<i>wide-l1</i>	Wide level-1 only.
<i>wide-l2</i>	Wide level-2 only.
<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.
<i>wide-transition-l1</i>	Wide-transition level-1 only.
<i>wide-transition-l2</i>	Wide-transition level-2 only.
<i>transition-l1</i>	Transition level-1 only.
<i>transition-l2</i>	Transition level-2 only.

Parameter	Description	Type	Size
overload-bit	Enable/disable signal other routers not to use us in SPF.	option	-
	Option	Description	
	<i>enable</i>	Enable overload bit.	
	<i>disable</i>	Disable overload bit.	
overload-bit-on-startup	Overload-bit only temporarily after reboot.	integer	Minimum value: 5 Maximum value: 86400
overload-bit-suppress	Suppress overload-bit for the specific prefixes.	option	-
	Option	Description	
	<i>external</i>	External.	
	<i>interlevel</i>	Inter-level.	
redistribute-l1	Enable/disable redistribution of level 1 routes into level 2.	option	-
	Option	Description	
	<i>enable</i>	Enable redistribution of level 1 routes into level 2.	
	<i>disable</i>	Disable redistribution of level 1 routes into level 2.	
redistribute-l1-list	Access-list for route redistribution from l1 to l2.	string	Maximum length: 35
redistribute-l2	Enable/disable redistribution of level 2 routes into level 1.	option	-
	Option	Description	
	<i>enable</i>	Enable redistribution of level 2 routes into level 1.	
	<i>disable</i>	Disable redistribution of level 2 routes into level 1.	
redistribute-l2-list	Access-list for route redistribution from l2 to l1.	string	Maximum length: 35
redistribute6-l1	Enable/disable redistribution of level 1 IPv6 routes into level 2.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable redistribution of level 1 IPv6 routes into level 2.	
	<i>disable</i>	Disable redistribution of level 1 IPv6 routes into level 2.	
redistribute6-l1-list	Access-list for IPv6 route redistribution from l1 to l2.	string	Maximum length: 35
redistribute6-l2	Enable/disable redistribution of level 2 IPv6 routes into level 1.	option	-
	Option	Description	
	<i>enable</i>	Enable redistribution of level 2 IPv6 routes into level 1.	
	<i>disable</i>	Disable redistribution of level 2 IPv6 routes into level 1.	
redistribute6-l2-list	Access-list for IPv6 route redistribution from l2 to l1.	string	Maximum length: 35
spf-interval-exp-l1	Level 1 SPF calculation delay.	user	Not Specified
spf-interval-exp-l2	Level 2 SPF calculation delay.	user	Not Specified

config isis-interface

Parameter	Description	Type	Size						
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35						
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35						
auth-mode-l1	Level 1 authentication mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>password</i></td><td>Password.</td></tr></table>			Option	Description	<i>md5</i>	MD5.	<i>password</i>	Password.
Option	Description								
<i>md5</i>	MD5.								
<i>password</i>	Password.								
auth-mode-l2	Level 2 authentication mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>password</i></td><td>Password.</td></tr></table>			Option	Description	<i>md5</i>	MD5.	<i>password</i>	Password.
Option	Description								
<i>md5</i>	MD5.								
<i>password</i>	Password.								

Parameter	Description	Type	Size
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified
auth-send-only-l1	Enable/disable authentication send-only for level 1 PDUs.	option	-
	Option	Description	
	<i>enable</i>	Enable authentication send-only for level 1 PDUs.	
	<i>disable</i>	Disable authentication send-only for level 1 PDUs.	
auth-send-only-l2	Enable/disable authentication send-only for level 2 PDUs.	option	-
	Option	Description	
	<i>enable</i>	Enable authentication send-only for level 2 PDUs.	
	<i>disable</i>	Disable authentication send-only for level 2 PDUs.	
circuit-type	IS-IS interface's circuit type	option	-
	Option	Description	
	<i>level-1-2</i>	Level 1 and 2.	
	<i>level-1</i>	Level 1.	
	<i>level-2</i>	Level 2.	
csnp-interval-l1	Level 1 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535
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

Parameter	Description	Type	Size						
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable padding to IS-IS hello packets.</td></tr><tr><td><i>disable</i></td><td>Disable padding to IS-IS hello packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable padding to IS-IS hello packets.	<i>disable</i>	Disable padding to IS-IS hello packets.		
Option	Description								
<i>enable</i>	Enable padding to IS-IS hello packets.								
<i>disable</i>	Disable padding to IS-IS hello packets.								
lsp-interval	LSP transmission interval (milliseconds).	integer	Minimum value: 1 Maximum value: 4294967295						
lsp-retransmit-interval	LSP retransmission interval (sec).	integer	Minimum value: 1 Maximum value: 65535						
mesh-group	Enable/disable IS-IS mesh group.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IS-IS mesh group.</td></tr><tr><td><i>disable</i></td><td>Disable IS-IS mesh group.</td></tr></table>	Option	Description	<i>enable</i>	Enable IS-IS mesh group.	<i>disable</i>	Disable IS-IS mesh group.		
Option	Description								
<i>enable</i>	Enable IS-IS mesh group.								
<i>disable</i>	Disable IS-IS mesh group.								
mesh-group-id	Mesh group ID <0-4294967295>, 0: mesh-group blocked.	integer	Minimum value: 0 Maximum value: 4294967295						
metric-l1	Level 1 metric for interface.	integer	Minimum value: 1 Maximum value: 63						

Parameter	Description	Type	Size
metric-l2	Level 2 metric for interface.	integer	Minimum value: 1 Maximum value: 63
name	IS-IS interface name.	string	Maximum length: 15
network-type	IS-IS interface's network type	option	-

Option	Description
<i>broadcast</i>	Broadcast.
<i>point-to-point</i>	Point-to-point.
<i>loopback</i>	Loopback.

priority-l1	Level 1 priority.	integer	Minimum value: 0 Maximum value: 127
priority-l2	Level 2 priority.	integer	Minimum value: 0 Maximum value: 127
status	Enable/disable interface for IS-IS.	option	-

Option	Description
<i>enable</i>	Enable interface for IS-IS.
<i>disable</i>	Disable interface for IS-IS.

status6	Enable/disable IPv6 interface for IS-IS.	option	-

Option	Description
<i>enable</i>	Enable IPv6 interface for IS-IS.
<i>disable</i>	Disable IPv6 interface for IS-IS.

wide-metric-l1	Level 1 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214

Parameter	Description	Type	Size
wide-metric-l2	Level 2 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214

config isis-net

Parameter	Description	Type	Size
id	isis-net ID.	integer	Minimum value: 0 Maximum value: 4294967295
net	IS-IS net xx.xxxx. xxxx.xx.	user	Not Specified

config redistribute

Parameter	Description	Type	Size
level	Level.	option	-
	Option	Description	
	level-1-2	Level 1 and 2.	
	level-1	Level 1.	
	level-2	Level 2.	
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864
metric-type	Metric type.	option	-
	Option	Description	
	external	External.	
	internal	Internal.	
protocol	Protocol name.	string	Maximum length: 35

Parameter	Description	Type	Size						
route-map	Route map name.	string	Maximum length: 35						
status	Status.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable.</td></tr><tr><td><i>disable</i></td><td>Disable.</td></tr></table>			Option	Description	<i>enable</i>	Enable.	<i>disable</i>	Disable.
	Option	Description							
	<i>enable</i>	Enable.							
<i>disable</i>	Disable.								

config redistribute6

Parameter	Description	Type	Size								
level	Level.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>level-1-2</i></td><td>Level 1 and 2.</td></tr><tr><td><i>level-1</i></td><td>Level 1.</td></tr><tr><td><i>level-2</i></td><td>Level 2.</td></tr></table>	Option	Description	<i>level-1-2</i>	Level 1 and 2.	<i>level-1</i>	Level 1.	<i>level-2</i>	Level 2.		
	Option	Description									
	<i>level-1-2</i>	Level 1 and 2.									
	<i>level-1</i>	Level 1.									
<i>level-2</i>	Level 2.										
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864								
metric-type	Metric type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external</i></td><td>External metric type.</td></tr><tr><td><i>internal</i></td><td>Internal metric type.</td></tr></table>	Option	Description	<i>external</i>	External metric type.	<i>internal</i>	Internal metric type.				
	Option	Description									
	<i>external</i>	External metric type.									
<i>internal</i>	Internal metric type.										
protocol	Protocol name.	string	Maximum length: 35								
routemap	Route map name.	string	Maximum length: 35								
status	Enable/disable redistribution.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribution.</td></tr><tr><td><i>disable</i></td><td>Disable redistribution.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribution.	<i>disable</i>	Disable redistribution.				
	Option	Description									
	<i>enable</i>	Enable redistribution.									
<i>disable</i>	Disable redistribution.										

config summary-address

Parameter	Description	Type	Size								
id	Summary address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295								
level	Level.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>level-1-2</td><td>Level 1 and 2.</td></tr><tr><td>level-1</td><td>Level 1.</td></tr><tr><td>level-2</td><td>Level 2.</td></tr></table>			Option	Description	level-1-2	Level 1 and 2.	level-1	Level 1.	level-2	Level 2.
	Option	Description									
	level-1-2	Level 1 and 2.									
	level-1	Level 1.									
level-2	Level 2.										
prefix	Prefix.	ipv4-classnet-any	Not Specified								

config summary-address6

Parameter	Description	Type	Size
id	Prefix entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
level	Level.	option	-
	Option	Description	
	level-1-2	Level 1 and 2.	
	level-1	Level 1.	
	level-2	Level 2.	
prefix6	IPv6 prefix.	ipv6-prefix	Not Specified

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 key-string {string}
            set send-lifetime {user}
        next
    end
next
end

```

config router key-chain

Parameter	Description	Type	Size
name	Key-chain name.	string	Maximum length: 35

config key

Parameter	Description	Type	Size
accept-lifetime	Lifetime of received authentication key (format: hh:mm:ss day month year).	user	Not Specified
id	Key ID (0 - 2147483647).	string	Maximum length: 10
key-string	Password for the key (max. = 35 characters).	string	Maximum length: 35
send-lifetime	Lifetime of sent authentication key (format: hh:mm:ss day month year).	user	Not Specified

config router multicast

Configure router multicast.

```

config router multicast
    Description: Configure router multicast.
    config interface
        Description: PIM interfaces.
        edit <name>
            set bfd [enable|disable]
            set cisco-exclude-genid [enable|disable]
            set dr-priority {integer}
            set hello-holdtime {integer}
            set hello-interval {integer}
        config igmp
            Description: IGMP configuration options.
            set access-group {string}
            set immediate-leave-group {string}
        end
    end
end

```

```

        set last-member-query-count {integer}
        set last-member-query-interval {integer}
        set query-interval {integer}
        set query-max-response-time {integer}
        set query-timeout {integer}
        set router-alert-check [enable|disable]
        set version [3|2|...]
    end
    config join-group
        Description: Join multicast groups.
        edit <address>
            next
        end
        set multicast-flow {string}
        set neighbour-filter {string}
        set passive [enable|disable]
        set pim-mode [sparse-mode|dense-mode]
        set propagation-delay {integer}
        set rp-candidate [enable|disable]
        set rp-candidate-group {string}
        set rp-candidate-interval {integer}
        set rp-candidate-priority {integer}
        set rpf-nbr-fail-back [enable|disable]
        set rpf-nbr-fail-back-filter {string}
        set state-refresh-interval {integer}
        set static-group {string}
        set ttl-threshold {integer}
    next
end
set multicast-routing [enable|disable]
config pim-sm-global
    Description: PIM sparse-mode global settings.
    set accept-register-list {string}
    set accept-source-list {string}
    set bsr-allow-quick-refresh [enable|disable]
    set bsr-candidate [enable|disable]
    set bsr-hash {integer}
    set bsr-interface {string}
    set bsr-priority {integer}
    set cisco-crp-prefix [enable|disable]
    set cisco-ignore-rp-set-priority [enable|disable]
    set cisco-register-checksum [enable|disable]
    set cisco-register-checksum-group {string}
    set join-prune-holdtime {integer}
    set message-interval {integer}
    set null-register-retries {integer}
    set register-rate-limit {integer}
    set register-rp-reachability [enable|disable]
    set register-source [disable|interface|...]
    set register-source-interface {string}
    set register-source-ip {ipv4-address}
    set register-supression {integer}
    config rp-address
        Description: Statically configure RP addresses.
        edit <id>
            set group {string}

```



```

        set ip-address {ipv4-address}
    next
end
set rp-register-keepalive {integer}
set spt-threshold [enable|disable]
set spt-threshold-group {string}
set ssm [enable|disable]
set ssm-range {string}
end
set route-limit {integer}
set route-threshold {integer}
end

```

config router multicast

Parameter	Description	Type	Size
multicast-routing	Enable/disable IP multicast routing.	option	-
	Option	Description	
	<i>enable</i>	Enable IP multicast routing.	
	<i>disable</i>	Disable IP multicast routing.	
route-limit	Maximum number of multicast routes.	integer	Minimum value: 1 Maximum value: 2147483647
route-threshold	Generate warnings when the number of multicast routes exceeds this number, must not be greater than route-limit.	integer	Minimum value: 1 Maximum value: 2147483647

config interface

Parameter	Description	Type	Size
bfd	Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	option	-
	Option	Description	
	<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	
	<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	

Parameter	Description	Type	Size
cisco-exclude-genid	Exclude GenID from hello packets (compatibility with old Cisco IOS).	option	-
	Option	Description	
	<i>enable</i>	Do not send GenID.	
	<i>disable</i>	Send GenID according to standard.	
dr-priority	DR election priority.	integer	Minimum value: 1 Maximum value: 4294967295
hello-holdtime	Time before old neighbor information expires (0 - 65535 sec, default = 105).	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Interval between sending PIM hello messages (0 - 65535 sec, default = 30).	integer	Minimum value: 1 Maximum value: 65535
multicast-flow	Acceptable source for multicast group.	string	Maximum length: 35
name	Interface name.	string	Maximum length: 15
neighbour-filter	Routers acknowledged as neighbor routers.	string	Maximum length: 35
passive	Enable/disable listening to IGMP but not participating in PIM.	option	-
	Option	Description	
	<i>enable</i>	Listen only.	
	<i>disable</i>	Participate in PIM.	
pim-mode	PIM operation mode.	option	-
	Option	Description	
	<i>sparse-mode</i>	sparse-mode	
	<i>dense-mode</i>	dense-mode	

Parameter	Description	Type	Size						
propagation-delay	Delay flooding packets on this interface (100 - 5000 msec, default = 500).	integer	Minimum value: 100 Maximum value: 5000						
rp-candidate	Enable/disable compete to become RP in elections.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Compete for RP elections.</td></tr><tr><td><i>disable</i></td><td>Do not compete for RP elections.</td></tr></table>	Option	Description	<i>enable</i>	Compete for RP elections.	<i>disable</i>	Do not compete for RP elections.		
Option	Description								
<i>enable</i>	Compete for RP elections.								
<i>disable</i>	Do not compete for RP elections.								
rp-candidate-group	Multicast groups managed by this RP.	string	Maximum length: 35						
rp-candidate-interval	RP candidate advertisement interval (1 - 16383 sec, default = 60).	integer	Minimum value: 1 Maximum value: 16383						
rp-candidate-priority	Router's priority as RP.	integer	Minimum value: 0 Maximum value: 255						
rpf-nbr-fail-back	Enable/disable fail back for RPF neighbor query.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fail back for RPF neighbor query.</td></tr><tr><td><i>disable</i></td><td>Disable fail back for RPF neighbor query.</td></tr></table>	Option	Description	<i>enable</i>	Enable fail back for RPF neighbor query.	<i>disable</i>	Disable fail back for RPF neighbor query.		
Option	Description								
<i>enable</i>	Enable fail back for RPF neighbor query.								
<i>disable</i>	Disable fail back for RPF neighbor query.								
rpf-nbr-fail-back-filter	Filter for fail back RPF neighbors.	string	Maximum length: 35						
state-refresh-interval	Interval between sending state-refresh packets (1 - 100 sec, default = 60).	integer	Minimum value: 1 Maximum value: 100						
static-group	Statically set multicast groups to forward out.	string	Maximum length: 35						
ttl-threshold	Minimum TTL of multicast packets that will be forwarded (applied only to new multicast routes) (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255						

config igmp

Parameter	Description	Type	Size
access-group	Groups IGMP hosts are allowed to join.	string	Maximum length: 35
immediate-leave-group	Groups to drop membership for immediately after receiving IGMPv2 leave.	string	Maximum length: 35
last-member-query-count	Number of group specific queries before removing group (2 - 7, default = 2).	integer	Minimum value: 2 Maximum value: 7
last-member-query-interval	Timeout between IGMPv2 leave and removing group (1 - 65535 msec, default = 1000).	integer	Minimum value: 1 Maximum value: 65535
query-interval	Interval between queries to IGMP hosts (1 - 65535 sec, default = 125).	integer	Minimum value: 1 Maximum value: 65535
query-max-response-time	Maximum time to wait for a IGMP query response (1 - 25 sec, default = 10).	integer	Minimum value: 1 Maximum value: 25
query-timeout	Timeout between queries before becoming querier for network (60 - 900, default = 255).	integer	Minimum value: 60 Maximum value: 900
router-alert-check	Enable/disable require IGMP packets contain router alert option.	option	-

Option	Description
<i>enable</i>	Require Router Alert option in IGMP packets.
<i>disable</i>	don't require Router Alert option in IGMP packets

Option	Description
3	Version 3 and lower.
2	Version 2 and lower.
1	Version 1.

config join-group

Parameter	Description	Type	Size
address	Multicast group IP address.	ipv4-address-any	Not Specified

config pim-sm-global

Parameter	Description	Type	Size						
accept-register-list	Sources allowed to register packets with this Rendezvous Point (RP).	string	Maximum length: 35						
accept-source-list	Sources allowed to send multicast traffic.	string	Maximum length: 35						
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow quick refresh packets.</td></tr><tr><td><i>disable</i></td><td>Do not allow quick refresh packets.</td></tr></table>			Option	Description	<i>enable</i>	Allow quick refresh packets.	<i>disable</i>	Do not allow quick refresh packets.
Option	Description								
<i>enable</i>	Allow quick refresh packets.								
<i>disable</i>	Do not allow quick refresh packets.								
bsr-candidate	Enable/disable allowing this router to become a bootstrap router (BSR).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow this router to function as a BSR.</td></tr><tr><td><i>disable</i></td><td>Do not allow this router to function as a BSR.</td></tr></table>			Option	Description	<i>enable</i>	Allow this router to function as a BSR.	<i>disable</i>	Do not allow this router to function as a BSR.
Option	Description								
<i>enable</i>	Allow this router to function as a BSR.								
<i>disable</i>	Do not allow this router to function as a BSR.								
bsr-hash	BSR hash length (0 - 32, default = 10).	integer	Minimum value: 0 Maximum value: 32						
bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15						
bsr-priority	BSR priority (0 - 255, default = 0).	integer	Minimum value: 0 Maximum value: 255						
cisco-crp-prefix	Enable/disable making candidate RP compatible with old Cisco IOS.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Do not allow sending group prefix of zero.	
	<i>disable</i>	Allow sending group prefix of zero.	
cisco-ignore-rp-set-priority	Use only hash for RP selection (compatibility with old Cisco IOS).	option	-
	Option	Description	
	<i>enable</i>	Ignore RP-SET priority value.	
	<i>disable</i>	Do not ignore RP-SET priority value.	
cisco-register-checksum	Checksum entire register packet(for old Cisco IOS compatibility).	option	-
	Option	Description	
	<i>enable</i>	register checksum entire packet.	
	<i>disable</i>	Do not register checksum entire packet.	
cisco-register-checksum-group	Cisco register checksum only these groups.	string	Maximum length: 35
join-prune-holdtime	Join/prune holdtime (1 - 65535, default = 210).	integer	Minimum value: 1 Maximum value: 65535
message-interval	Period of time between sending periodic PIM join/prune messages in seconds (1 - 65535, default = 60).	integer	Minimum value: 1 Maximum value: 65535
null-register-retries	Maximum retries of null register (1 - 20, default = 1).	integer	Minimum value: 1 Maximum value: 20
register-rate-limit	Limit of packets/sec per source registered through this RP (0 - 65535, default = 0 which means unlimited).	integer	Minimum value: 0 Maximum value: 65535
register-rp-reachability	Enable/disable check RP is reachable before registering packets.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check target RP is unicast reachable before registering.</td></tr><tr><td><i>disable</i></td><td>Do not check RP unicast reachability.</td></tr></table>	Option	Description	<i>enable</i>	Check target RP is unicast reachable before registering.	<i>disable</i>	Do not check RP unicast reachability.				
	Option	Description									
	<i>enable</i>	Check target RP is unicast reachable before registering.									
<i>disable</i>	Do not check RP unicast reachability.										
register-source	Override source address in register packets.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Use source address of RPF interface.</td></tr><tr><td><i>interface</i></td><td>Use primary IP of an interface.</td></tr><tr><td><i>ip-address</i></td><td>Use a local IP address.</td></tr></table>	Option	Description	<i>disable</i>	Use source address of RPF interface.	<i>interface</i>	Use primary IP of an interface.	<i>ip-address</i>	Use a local IP address.		
	Option	Description									
	<i>disable</i>	Use source address of RPF interface.									
	<i>interface</i>	Use primary IP of an interface.									
<i>ip-address</i>	Use a local IP address.										
register-source-interface	Override with primary interface address.	string	Maximum length: 15								
register-source-ip	Override with local IP address.	ipv4-address	Not Specified								
register-supression	Period of time to honor register-stop message (1 - 65535 sec, default = 60).	integer	Minimum value: 1 Maximum value: 65535								
rp-register-keepalive	Timeout for RP receiving data on (S,G) tree (1 - 65535 sec, default = 185).	integer	Minimum value: 1 Maximum value: 65535								
spt-threshold	Enable/disable switching to source specific trees.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Switch to Source tree when available.</td></tr><tr><td><i>disable</i></td><td>Do not switch to Source tree when available.</td></tr></table>	Option	Description	<i>enable</i>	Switch to Source tree when available.	<i>disable</i>	Do not switch to Source tree when available.				
	Option	Description									
	<i>enable</i>	Switch to Source tree when available.									
<i>disable</i>	Do not switch to Source tree when available.										
spt-threshold-group	Groups allowed to switch to source tree.	string	Maximum length: 35								
ssm	Enable/disable source specific multicast.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow source specific multicast.</td></tr><tr><td><i>disable</i></td><td>Do not allow source specific multicast.</td></tr></table>	Option	Description	<i>enable</i>	Allow source specific multicast.	<i>disable</i>	Do not allow source specific multicast.				
	Option	Description									
	<i>enable</i>	Allow source specific multicast.									
<i>disable</i>	Do not allow source specific multicast.										
ssm-range	Groups allowed to source specific multicast.	string	Maximum length: 35								

config rp-address

Parameter	Description	Type	Size
group	Groups to use this RP.	string	Maximum length: 35
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip-address	RP router address.	ipv4-address	Not Specified

config router multicast6

Configure IPv6 multicast.

```
config router multicast6
  Description: Configure IPv6 multicast.
  config interface
    Description: Protocol Independent Multicast (PIM) interfaces.
    edit <name>
      set hello-holdtime {integer}
      set hello-interval {integer}
    next
  end
  set multicast-pmtu [enable|disable]
  set multicast-routing [enable|disable]
  config pim-sm-global
    Description: PIM sparse-mode global settings.
    set 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-pmtu	Enable/disable PMTU for IPv6 multicast.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable PMTU for IPv6 multicast.	
	<i>disable</i>	Disable PMTU for IPv6 multicast.	
multicast-routing	Enable/disable IPv6 multicast routing.	option	-
	Option	Description	
	<i>enable</i>	Enable IPv6 multicast routing.	
	<i>disable</i>	Disable IPv6 multicast routing.	

config interface

Parameter	Description	Type	Size
hello-holdtime	Time before old neighbour information expires (1 - 65535 sec, default = 105).	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Interval between sending PIM hello messages (1 - 65535 sec, default = 30).	integer	Minimum value: 1 Maximum value: 65535
name	Interface name.	string	Maximum length: 15

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
id	ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295
ipv6-address	RP router IPv6 address.	ipv6-address	Not Specified

config router multicast-flow

Configure multicast-flow.

```
config router multicast-flow
  Description: Configure multicast-flow.
  edit <name>
    set comments {string}
    config flows
      Description: Multicast-flow entries.
      edit <id>
        set group-addr {ipv4-address-any}
        set source-addr {ipv4-address-any}
      next
    end
  next
end
```

config router multicast-flow

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

config flows

Parameter	Description	Type	Size
group-addr	Multicast group IP address.	ipv4-address-any	Not Specified

Parameter	Description	Type	Size
id	Flow ID.	integer	Minimum value: 0 Maximum value: 4294967295
source-addr	Multicast source IP address.	ipv4-address-any	Not Specified

config router ospf

Configure OSPF.

```

config router ospf
  Description: Configure OSPF.
  set abr-type [cisco|ibm|...]
  config area
    Description: OSPF area configuration.
    edit <id>
      set authentication [none|text|...]
      set default-cost {integer}
      config filter-list
        Description: OSPF area filter-list configuration.
        edit <id>
          set direction [in|out]
          set list {string}
        next
      end
      set nssa-default-information-originate [enable|always|...]
      set nssa-default-information-originate-metric {integer}
      set nssa-default-information-originate-metric-type [1|2]
      set nssa-redistribution [enable|disable]
      set nssa-translator-role [candidate|never|...]
      config range
        Description: OSPF area range configuration.
        edit <id>
          set advertise [disable|enable]
          set prefix {ipv4-classnet-any}
          set substitute {ipv4-classnet-any}
          set substitute-status [enable|disable]
        next
      end
      set shortcut [disable|enable|...]
      set stub-type [no-summary|summary]
      set type [regular|nssa|...]
      config virtual-link
        Description: OSPF virtual link configuration.
        edit <name>
          set authentication [none|text|...]
          set authentication-key {password}
          set dead-interval {integer}

```

```

        set hello-interval {integer}
        set md5-keychain {string}
        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end
        set peer {ipv4-address-any}
        set retransmit-interval {integer}
        set transmit-delay {integer}
    next
end
next
end
set auto-cost-ref-bandwidth {integer}
set bfd [enable|disable]
set database-overflow [enable|disable]
set database-overflow-max-lsas {integer}
set database-overflow-time-to-recover {integer}
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-originate [enable|always|...]
set default-information-route-map {string}
set default-metric {integer}
set distance {integer}
set distance-external {integer}
set distance-inter-area {integer}
set distance-intra-area {integer}
config distribute-list
    Description: Distribute list configuration.
    edit <id>
        set access-list {string}
        set protocol [connected|static|...]
    next
end
set distribute-list-in {string}
set distribute-route-map-in {string}
set log-neighbour-changes [enable|disable]
config neighbor
    Description: OSPF neighbor configuration are used when OSPF runs on non-broadcast
media
    edit <id>
        set cost {integer}
        set ip {ipv4-address}
        set poll-interval {integer}
        set priority {integer}
    next
end
config network
    Description: OSPF network configuration.
    edit <id>
        set area {ipv4-address-any}
        set prefix {ipv4-classnet}
    next
end

```

```

config ospf-interface
    Description: OSPF interface configuration.
    edit <name>
        set authentication [none|text|...]
        set authentication-key {password}
        set bfd [global|enable|...]
        set cost {integer}
        set database-filter-out [enable|disable]
        set dead-interval {integer}
        set hello-interval {integer}
        set hello-multiplier {integer}
        set interface {string}
        set ip {ipv4-address}
        set md5-keychain {string}
        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end
        set mtu {integer}
        set mtu-ignore [enable|disable]
        set network-type [broadcast|non-broadcast|...]
        set prefix-length {integer}
        set priority {integer}
        set resync-timeout {integer}
        set retransmit-interval {integer}
        set status [disable|enable]
        set transmit-delay {integer}
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set metric-type [1|2]
        set routemap {string}
        set status [enable|disable]
        set tag {integer}
    next
end
set restart-mode [none|lls|...]
set restart-period {integer}
set rfc1583-compatible [enable|disable]
set router-id {ipv4-address-any}
set spf-timers {user}
config summary-address
    Description: IP address summary configuration.
    edit <id>
        set advertise [disable|enable]
        set prefix {ipv4-classnet}
        set tag {integer}
    next
end
end

```

config router ospf

Parameter	Description	Type	Size										
abr-type	Area border router type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cisco</td><td>Cisco.</td></tr><tr><td>ibm</td><td>IBM.</td></tr><tr><td>shortcut</td><td>Shortcut.</td></tr><tr><td>standard</td><td>Standard.</td></tr></table>	Option	Description	cisco	Cisco.	ibm	IBM.	shortcut	Shortcut.	standard	Standard.		
Option	Description												
cisco	Cisco.												
ibm	IBM.												
shortcut	Shortcut.												
standard	Standard.												
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000										
bfd	Bidirectional Forwarding Detection (BFD).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.						
Option	Description												
enable	Enable setting.												
disable	Disable setting.												
database-overflow	Enable/disable database overflow.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.						
Option	Description												
enable	Enable setting.												
disable	Disable setting.												
database-overflow-max-lsas	Database overflow maximum LSAs.	integer	Minimum value: 0 Maximum value: 4294967295										
database-overflow-time-to-recover	Database overflow time to recover (sec).	integer	Minimum value: 0 Maximum value: 65535										
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214										

Parameter	Description	Type	Size								
default-information-metric-type	Default information metric type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>			Option	Description	1	Type 1.	2	Type 2.		
Option	Description										
1	Type 1.										
2	Type 2.										
default-information-originate	Enable/disable generation of default route.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>always</i></td><td>Always advertise the default router.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>always</i>	Always advertise the default router.	<i>disable</i>	Disable setting.
Option	Description										
<i>enable</i>	Enable setting.										
<i>always</i>	Always advertise the default router.										
<i>disable</i>	Disable setting.										
default-information-route-map	Default information route map.	string	Maximum length: 35								
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214								
distance	Distance of the route.	integer	Minimum value: 1 Maximum value: 255								
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								

Parameter	Description	Type	Size
distribute-list-in	Filter incoming routes.	string	Maximum length: 35
distribute-route-map-in	Filter incoming external routes by route-map.	string	Maximum length: 35
log-neighbour-changes	Enable logging of OSPF neighbour's changes	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79
restart-mode	OSPF restart mode (graceful or LLS).	option	-

Option	Description
<i>none</i>	Hitless restart disabled.
<i>lls</i>	LLS mode.
<i>graceful-restart</i>	Graceful Restart Mode.

restart-period	Graceful restart period.	integer	Minimum value: 1 Maximum value: 3600
rfc1583-compatible	Enable/disable RFC1583 compatibility.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

router-id	Router ID.	ipv4-address-any	Not Specified
spf-timers	SPF calculation frequency.	user	Not Specified

config area

Parameter	Description	Type	Size
authentication	Authentication type.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	None.	
	<i>text</i>	Text.	
	<i>md5</i>	MD5.	
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 4294967295
id	Area entry IP address.	ipv4-address-any	Not Specified
nssa-default-information-originate	Redistribute, advertise, or do not originate Type-7 default route into NSSA area.	option	-
	Option	Description	
	<i>enable</i>	Redistribute Type-7 default route from routing table.	
	<i>always</i>	Advertise a self-originated Type-7 default route.	
	<i>disable</i>	Do not advertise Type-7 default route.	
nssa-default-information-originate-metric	OSPF default metric.	integer	Minimum value: 0 Maximum value: 16777214
nssa-default-information-originate-metric-type	OSPF metric type for default routes.	option	-
	Option	Description	
	<i>1</i>	Type 1.	
	<i>2</i>	Type 2.	
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable redistribute into NSSA area.	
	<i>disable</i>	Disable redistribute into NSSA area.	
nssa-translator-role	NSSA translator role type.	option	-
	Option	Description	
	<i>candidate</i>	Candidate.	
	<i>never</i>	Never.	
	<i>always</i>	Always.	
shortcut	Enable/disable shortcut option.	option	-
	Option	Description	
	<i>disable</i>	Disable shortcut option.	
	<i>enable</i>	Enable shortcut option.	
	<i>default</i>	Default shortcut option.	
stub-type	Stub summary setting.	option	-
	Option	Description	
	<i>no-summary</i>	No summary.	
	<i>summary</i>	Summary.	
type	Area type setting.	option	-
	Option	Description	
	<i>regular</i>	Regular.	
	<i>nssa</i>	NSSA.	
	<i>stub</i>	Stub.	

config filter-list

Parameter	Description	Type	Size
direction	Direction.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>in</i>	In.	
	<i>out</i>	Out.	
id	Filter list entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
list	Access-list or prefix-list name.	string	Maximum length: 35

config range

Parameter	Description	Type	Size						
advertise	Enable/disable advertise status.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable advertise status.</td></tr><tr><td><i>enable</i></td><td>Enable advertise status.</td></tr></table>			Option	Description	<i>disable</i>	Disable advertise status.	<i>enable</i>	Enable advertise status.
Option	Description								
<i>disable</i>	Disable advertise status.								
<i>enable</i>	Enable advertise status.								
id	Range entry ID.	integer	Minimum value: 0 Maximum value: 4294967295						
prefix	Prefix.	ipv4-classnet-any	Not Specified						
substitute	Substitute prefix.	ipv4-classnet-any	Not Specified						
substitute-status	Enable/disable substitute status.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable substitute status.</td></tr><tr><td><i>disable</i></td><td>Disable substitute status.</td></tr></table>			Option	Description	<i>enable</i>	Enable substitute status.	<i>disable</i>	Disable substitute status.
Option	Description								
<i>enable</i>	Enable substitute status.								
<i>disable</i>	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
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535
md5-keychain	Authentication MD5 key-chain name.	string	Maximum length: 35
name	Virtual link entry name.	string	Maximum length: 35
peer	Peer IP.	ipv4-address-any	Not Specified
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535

config md5-keys

Parameter	Description	Type	Size
id	Key ID (1 - 255).	integer	Minimum value: 1 Maximum value: 255

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

config distribute-list

Parameter	Description	Type	Size
access-list	Access list name.	string	Maximum length: 35
id	Distribute list entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
protocol	Protocol type.	option	-

Option	Description
<i>connected</i>	Connected type.
<i>static</i>	Static type.
<i>rip</i>	RIP type.

config neighbor

Parameter	Description	Type	Size
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
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
priority	Priority.	integer	Minimum value: 0 Maximum value: 255

config network

Parameter	Description	Type	Size
area	Attach the network to area.	ipv4-address-any	Not Specified
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix	Prefix.	ipv4-classnet	Not Specified

config ospf-interface

Parameter	Description	Type	Size								
authentication	Authentication type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>md5</i></td><td>MD5.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>md5</i>	MD5.		
Option	Description										
<i>none</i>	None.										
<i>text</i>	Text.										
<i>md5</i>	MD5.										
authentication-key	Authentication key.	password	Not Specified								
bfd	Bidirectional Forwarding Detection (BFD).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Follow global configuration.</td></tr><tr><td><i>enable</i></td><td>Enable BFD on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable BFD on this interface.</td></tr></table>	Option	Description	<i>global</i>	Follow global configuration.	<i>enable</i>	Enable BFD on this interface.	<i>disable</i>	Disable BFD on this interface.		
Option	Description										
<i>global</i>	Follow global configuration.										
<i>enable</i>	Enable BFD on this interface.										
<i>disable</i>	Disable BFD on this interface.										
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535								
database-filter-out	Enable/disable control of flooding out LSAs.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										

Parameter	Description	Type	Size
dead-interval	Dead interval.	integer	Minimum value: 0 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 0 Maximum value: 65535
hello-multiplier	Number of hello packets within dead interval.	integer	Minimum value: 3 Maximum value: 10
interface	Configuration interface name.	string	Maximum length: 15
ip	IP address.	ipv4-address	Not Specified
md5-keychain	Authentication MD5 key-chain name.	string	Maximum length: 35
mtu	MTU for database description packets.	integer	Minimum value: 576 Maximum value: 65535
mtu-ignore	Enable/disable ignore MTU.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

name	Interface entry name.	string	Maximum length: 35
network-type	Network type.	option	-

Option	Description
<i>broadcast</i>	Broadcast.
<i>non-broadcast</i>	Non-broadcast.
<i>point-to-point</i>	Point-to-point.
<i>point-to-multipoint</i>	Point-to-multipoint.

Parameter	Description	Type	Size
	Option	Description	
	<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.	
prefix-length	Prefix length.	integer	Minimum value: 0 Maximum value: 32
priority	Priority.	integer	Minimum value: 0 Maximum value: 255
resync-timeout	Graceful restart neighbor resynchronization timeout.	integer	Minimum value: 1 Maximum value: 3600
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable status.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535

config md5-keys

Parameter	Description	Type	Size
id	Key ID (1 - 255).	integer	Minimum value: 1 Maximum value: 255
key-string	Password for the key.	password	Not Specified

config redistribute

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

config summary-address

Parameter	Description	Type	Size
advertise	Enable/disable advertise status.	option	-
	Option	Description	
	<i>disable</i>	Disable advertise status.	
	<i>enable</i>	Enable advertise status.	

Parameter	Description	Type	Size
id	Summary address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix	Prefix.	ipv4-classnet	Not Specified
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|...]
  config area
    Description: OSPF6 area configuration.
    edit <id>
      set authentication [none|ah|...]
      set default-cost {integer}
      set ipsec-auth-alg [md5|sha1|...]
      set ipsec-enc-alg [null|des|...]
      config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
          set auth-key {password}
          set enc-key {password}
        next
      end
      set key-rollover-interval {integer}
      set nssa-default-information-originate [enable|disable]
      set nssa-default-information-originate-metric {integer}
      set nssa-default-information-originate-metric-type [1|2]
      set nssa-redistribution [enable|disable]
      set nssa-translator-role [candidate|never|...]
      config range
        Description: OSPF6 area range configuration.
        edit <id>
          set advertise [disable|enable]
          set prefix6 {ipv6-network}
        next
      end
      set stub-type [no-summary|summary]
      set type [regular|nssa|...]
      config virtual-link
```

```

Description: OSPF6 virtual link configuration.
edit <name>
    set authentication [none|ah|...]
    set dead-interval {integer}
    set hello-interval {integer}
    set ipsec-auth-alg [md5|sha1|...]
    set ipsec-enc-alg [null|des|...]
    config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
            set auth-key {password}
            set enc-key {password}
        next
    end
    set key-rollover-interval {integer}
    set peer {ipv4-address-any}
    set retransmit-interval {integer}
    set transmit-delay {integer}
next
end
next
end
set auto-cost-ref-bandwidth {integer}
set bfd [enable|disable]
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-originate [enable|always|...]
set default-information-route-map {string}
set default-metric {integer}
set log-neighbour-changes [enable|disable]
config ospf6-interface
    Description: OSPF6 interface configuration.
    edit <name>
        set area-id {ipv4-address-any}
        set authentication [none|ah|...]
        set bfd [global|enable|...]
        set cost {integer}
        set dead-interval {integer}
        set hello-interval {integer}
        set interface {string}
        set ipsec-auth-alg [md5|sha1|...]
        set ipsec-enc-alg [null|des|...]
        config ipsec-keys
            Description: IPsec authentication and encryption keys.
            edit <spi>
                set auth-key {password}
                set enc-key {password}
            next
        end
        set key-rollover-interval {integer}
        set mtu {integer}
        set mtu-ignore [enable|disable]
        config neighbor
            Description: OSPFv3 neighbors are used when OSPFv3 runs on non-broadcast
media
            edit <ip6>

```

```

        set cost {integer}
        set poll-interval {integer}
        set priority {integer}
    next
end
set network-type [broadcast|point-to-point|...]
set priority {integer}
set retransmit-interval {integer}
set status [disable|enable]
set transmit-delay {integer}
next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set metric-type [1|2]
        set routemap {string}
        set status [enable|disable]
    next
end
set router-id {ipv4-address-any}
set spf-timers {user}
config summary-address
    Description: IPv6 address summary configuration.
    edit <id>
        set advertise [disable|enable]
        set prefix6 {ipv6-network}
        set tag {integer}
    next
end
end
end

```

config router ospf6

Parameter	Description	Type	Size
abr-type	Area border router type.	option	-
	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

Parameter	Description	Type	Size
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-
	Option	Description	
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	
	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).	
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214
default-information-metric-type	Default information metric type.	option	-
	Option	Description	
	<i>1</i>	Type 1.	
	<i>2</i>	Type 2.	
default-information-originate	Enable/disable generation of default route.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>always</i>	Always advertise the default router.	
	<i>disable</i>	Disable setting.	
default-information-route-map	Default information route map.	string	Maximum length: 35
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214
log-neighbour-changes	Enable logging of OSPFv3 neighbour's changes	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79
router-id	A.B.C.D, in IPv4 address format.	ipv4-address- any	Not Specified
spf-timers	SPF calculation frequency.	user	Not Specified

config area

Parameter	Description	Type	Size
authentication	Authentication mode.	option	-
	Option	Description	
	<i>none</i>	Disable authentication.	
	<i>ah</i>	Authentication Header.	
	<i>esp</i>	Encapsulating Security Payload.	
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 16777215
id	Area entry IP address.	ipv4- address-any	Not Specified
ipsec-auth-alg	Authentication algorithm.	option	-
	Option	Description	
	<i>md5</i>	MD5.	
	<i>sha1</i>	SHA1.	
	<i>sha256</i>	SHA256.	
	<i>sha384</i>	SHA384.	
	<i>sha512</i>	SHA512.	
ipsec-enc-alg	Encryption algorithm.	option	-

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>No encryption.</td></tr><tr><td><i>des</i></td><td>DES.</td></tr><tr><td><i>3des</i></td><td>3DES.</td></tr><tr><td><i>aes128</i></td><td>AES128.</td></tr><tr><td><i>aes192</i></td><td>AES192.</td></tr><tr><td><i>aes256</i></td><td>AES256.</td></tr></table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.		
	Option	Description															
	<i>null</i>	No encryption.															
	<i>des</i>	DES.															
	<i>3des</i>	3DES.															
	<i>aes128</i>	AES128.															
	<i>aes192</i>	AES192.															
<i>aes256</i>	AES256.																
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000														
nssa-default-information-originate	Enable/disable originate type 7 default into NSSA area.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable originate type 7 default into NSSA area.</td></tr><tr><td><i>disable</i></td><td>Disable originate type 7 default into NSSA area.</td></tr></table>	Option	Description	<i>enable</i>	Enable originate type 7 default into NSSA area.	<i>disable</i>	Disable originate type 7 default into NSSA area.										
	Option	Description															
	<i>enable</i>	Enable originate type 7 default into NSSA area.															
<i>disable</i>	Disable originate type 7 default into NSSA area.																
nssa-default-information-originate-metric	OSPFv3 default metric.	integer	Minimum value: 0 Maximum value: 16777214														
nssa-default-information-originate-metric-type	OSPFv3 metric type for default routes.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1</i></td><td>Type 1.</td></tr><tr><td><i>2</i></td><td>Type 2.</td></tr></table>	Option	Description	<i>1</i>	Type 1.	<i>2</i>	Type 2.										
	Option	Description															
	<i>1</i>	Type 1.															
<i>2</i>	Type 2.																
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribute into NSSA area.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribute into NSSA area.												
	Option	Description															
<i>enable</i>	Enable redistribute into NSSA area.																

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable redistribute into NSSA area.	
	<i>nssa-translator-role</i>	NSSA translator role type.	option -
	Option	Description	
	<i>candidate</i>	Candidate.	
	<i>never</i>	Never.	
	<i>always</i>	Always.	
stub-type	Stub summary setting.	option	-
	Option	Description	
	<i>no-summary</i>	No summary.	
	<i>summary</i>	Summary.	
	Option	Description	
type	Area type setting.	option	-
	Option	Description	
	<i>regular</i>	Regular.	
	<i>nssa</i>	NSSA.	
	<i>stub</i>	Stub.	

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295

config range

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

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	disable	
	<i>enable</i>	enable	
id	Range entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	IPv6 prefix.	ipv6-network	Not Specified

config virtual-link

Parameter	Description	Type	Size
authentication	Authentication mode.	option	-
	Option	Description	
	<i>none</i>	Disable authentication.	
	<i>ah</i>	Authentication Header.	
	<i>esp</i>	Encapsulating Security Payload.	
	<i>area</i>	Use the routing area's authentication configuration.	
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535
ipsec-auth-alg	Authentication algorithm.	option	-
	Option	Description	
	<i>md5</i>	MD5.	
	<i>sha1</i>	SHA1.	
	<i>sha256</i>	SHA256.	
	<i>sha384</i>	SHA384.	
	<i>sha512</i>	SHA512.	

Parameter	Description	Type	Size														
ipsec-enc-alg	Encryption algorithm.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>No encryption.</td></tr><tr><td><i>des</i></td><td>DES.</td></tr><tr><td><i>3des</i></td><td>3DES.</td></tr><tr><td><i>aes128</i></td><td>AES128.</td></tr><tr><td><i>aes192</i></td><td>AES192.</td></tr><tr><td><i>aes256</i></td><td>AES256.</td></tr></table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.		
	Option	Description															
	<i>null</i>	No encryption.															
	<i>des</i>	DES.															
	<i>3des</i>	3DES.															
	<i>aes128</i>	AES128.															
	<i>aes192</i>	AES192.															
<i>aes256</i>	AES256.																
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000														
name	Virtual link entry name.	string	Maximum length: 35														
peer	A.B.C.D, peer router ID.	ipv4-address-any	Not Specified														
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535														
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535														

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295

config ospf6-interface

Parameter	Description	Type	Size
area-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified
authentication	Authentication mode.	option	-
	Option	Description	
	<i>none</i>	Disable authentication.	
	<i>ah</i>	Authentication Header.	
	<i>esp</i>	Encapsulating Security Payload.	
	<i>area</i>	Use the routing area's authentication configuration.	
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-
	Option	Description	
	<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).	
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.	
	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.	
	cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535
interface	Configuration interface name.	string	Maximum length: 15
ipsec-auth-alg	Authentication algorithm.	option	-
	Option	Description	
	<i>md5</i>	MD5.	
	<i>sha1</i>	SHA1.	

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>SHA256.</td></tr><tr><td>sha384</td><td>SHA384.</td></tr><tr><td>sha512</td><td>SHA512.</td></tr></table>	Option	Description	sha256	SHA256.	sha384	SHA384.	sha512	SHA512.								
	Option	Description															
	sha256	SHA256.															
	sha384	SHA384.															
	sha512	SHA512.															
ipsec-enc-alg	Encryption algorithm.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>No encryption.</td></tr><tr><td>des</td><td>DES.</td></tr><tr><td>3des</td><td>3DES.</td></tr><tr><td>aes128</td><td>AES128.</td></tr><tr><td>aes192</td><td>AES192.</td></tr><tr><td>aes256</td><td>AES256.</td></tr></table>	Option	Description	null	No encryption.	des	DES.	3des	3DES.	aes128	AES128.	aes192	AES192.	aes256	AES256.		
	Option	Description															
	null	No encryption.															
	des	DES.															
	3des	3DES.															
	aes128	AES128.															
	aes192	AES192.															
aes256	AES256.																
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000														
mtu	MTU for OSPFv3 packets.	integer	Minimum value: 576 Maximum value: 65535														
mtu-ignore	Enable/disable ignoring MTU field in DBD packets.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Ignore MTU field in DBD packets.</td></tr><tr><td>disable</td><td>Do not ignore MTU field in DBD packets.</td></tr></table>	Option	Description	enable	Ignore MTU field in DBD packets.	disable	Do not ignore MTU field in DBD packets.										
	Option	Description															
	enable	Ignore MTU field in DBD packets.															
disable	Do not ignore MTU field in DBD packets.																
name	Interface entry name.	string	Maximum length: 35														
network-type	Network type.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>broadcast</td><td>broadcast</td></tr><tr><td>point-to-point</td><td>point-to-point</td></tr><tr><td>non-broadcast</td><td>non-broadcast</td></tr></table>	Option	Description	broadcast	broadcast	point-to-point	point-to-point	non-broadcast	non-broadcast								
	Option	Description															
	broadcast	broadcast															
	point-to-point	point-to-point															
non-broadcast	non-broadcast																

Parameter	Description	Type	Size
	Option	Description	
	<i>point-to-multipoint</i>	point-to-multipoint	
	<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.	
priority	priority	integer	Minimum value: 0 Maximum value: 255
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable OSPF6 routing on this interface.	option	-
	Option	Description	
	<i>disable</i>	Disable OSPF6 routing.	
	<i>enable</i>	Enable OSPF6 routing.	
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535

config ipsec-keys

Parameter	Description	Type	Size
auth-key	Authentication key.	password	Not Specified
enc-key	Encryption key.	password	Not Specified
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295

config neighbor

Parameter	Description	Type	Size
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535
ip6	IPv6 link local address of the neighbor.	ipv6-address	Not Specified
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535
priority	priority	integer	Minimum value: 0 Maximum value: 255

config redistribute

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

config summary-address

Parameter	Description	Type	Size
advertise	Enable/disable advertise status.	option	-
	Option	Description	
	disable	disable	
	enable	enable	
id	Summary address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	IPv6 prefix.	ipv6-network	Not Specified
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295

config router policy

Configure IPv4 routing policies.

```
config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set action [deny|permit]
    set comments {var-string}
    set dst <subnet1>, <subnet2>, ...
    set dst-negate [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set end-port {integer}
    set end-source-port {integer}
    set gateway {ipv4-address}
    set input-device <name1>, <name2>, ...
    set input-device-negate [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-id <id1>, <id2>, ...
    set output-device {string}
    set protocol {integer}
    set src <subnet1>, <subnet2>, ...
    set src-negate [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set start-port {integer}
    set start-source-port {integer}
    set status [enable|disable]
```

```

        set tos {user}
        set tos-mask {user}
    next
end

```

config router policy

Parameter	Description	Type	Size						
action	Action of the policy route.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Do not search policy route table.</td></tr><tr><td><i>permit</i></td><td>Use this policy route for forwarding.</td></tr></table>	Option	Description	<i>deny</i>	Do not search policy route table.	<i>permit</i>	Use this policy route for forwarding.		
Option	Description								
<i>deny</i>	Do not search policy route table.								
<i>permit</i>	Use this policy route for forwarding.								
comments	Optional comments.	var-string	Maximum length: 255						
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79						
dst-negate	Enable/disable negating destination address match.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable destination address negation.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negation.</td></tr></table>	Option	Description	<i>enable</i>	Enable destination address negation.	<i>disable</i>	Disable destination address negation.		
Option	Description								
<i>enable</i>	Enable destination address negation.								
<i>disable</i>	Disable destination address negation.								
dstaddr <name>	Destination address name. Address/group name.	string	Maximum length: 79						
end-port	End destination port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535						
end-source-port	End source port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535						
gateway	IP address of the gateway.	ipv4-address	Not Specified						
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79						
input-device-negate	Enable/disable negation of input device match.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negation of input device match.</td></tr><tr><td><i>disable</i></td><td>Disable negation of input device match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negation of input device match.	<i>disable</i>	Disable negation of input device match.		
	Option	Description							
	<i>enable</i>	Enable negation of input device match.							
<i>disable</i>	Disable negation of input device match.								
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79						
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295						
output-device	Outgoing interface name.	string	Maximum length: 35						
protocol	Protocol number (0 - 255).	integer	Minimum value: 0 Maximum value: 255						
seq-num	Sequence number(1-65535).	integer	Minimum value: 1 Maximum value: 65535						
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79						
src-negate	Enable/disable negating source address match.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negation.</td></tr><tr><td><i>disable</i></td><td>Disable source address negation.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negation.	<i>disable</i>	Disable source address negation.		
	Option	Description							
	<i>enable</i>	Enable source address negation.							
<i>disable</i>	Disable source address negation.								
srcaddr <name>	Source address name. Address/group name.	string	Maximum length: 79						
start-port	Start destination port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535						

Parameter	Description	Type	Size						
start-source-port	Start source port number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535						
status	Enable/disable this policy route.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy route.</td></tr><tr><td><i>disable</i></td><td>Disable this policy route.</td></tr></table>			Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.
	Option	Description							
	<i>enable</i>	Enable this policy route.							
	<i>disable</i>	Disable this policy route.							
tos	Type of service bit pattern.	user	Not Specified						
tos-mask	Type of service evaluated bits.	user	Not Specified						

config router policy6

Configure IPv6 routing policies.

```

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

```

config router policy6

Parameter	Description	Type	Size
comments	Optional comments.	var-string	Maximum length: 255
dst	Destination IPv6 prefix.	ipv6-network	Not Specified

Parameter	Description	Type	Size						
end-port	End destination port number (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535						
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified						
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79						
output-device	Outgoing interface name.	string	Maximum length: 35						
protocol	Protocol number (0 - 255).	integer	Minimum value: 0 Maximum value: 255						
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295						
src	Source IPv6 prefix.	ipv6-network	Not Specified						
start-port	Start destination port number (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535						
status	Enable/disable this policy route.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy route.</td></tr><tr><td><i>disable</i></td><td>Disable this policy route.</td></tr></table>	Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.		
Option	Description								
<i>enable</i>	Enable this policy route.								
<i>disable</i>	Disable this policy route.								
tos	Type of service bit pattern.	user	Not Specified						
tos-mask	Type of service evaluated bits.	user	Not Specified						

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 flags {integer}
    set ge {integer}
    set le {integer}
    set prefix {user}
next
end
next
end

```

config router prefix-list

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

config rule

Parameter	Description	Type	Size						
action	Permit or deny this IP address and netmask prefix.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>permit</i></td><td>Allow or permit packets that match this rule.</td></tr><tr><td><i>deny</i></td><td>Deny packets that match this rule.</td></tr></table>	Option	Description	<i>permit</i>	Allow or permit packets that match this rule.	<i>deny</i>	Deny packets that match this rule.		
Option	Description								
<i>permit</i>	Allow or permit packets that match this rule.								
<i>deny</i>	Deny packets that match this rule.								
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295						
ge	Minimum prefix length to be matched (0 - 32).	integer	Minimum value: 0 Maximum value: 32						
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295						

Parameter	Description	Type	Size
le	Maximum prefix length to be matched (0 - 32).	integer	Minimum value: 0 Maximum value: 32
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified

config router prefix-list6

Configure IPv6 prefix lists.

```

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

```

config router prefix-list6

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

config rule

Parameter	Description	Type	Size
action	Permit or deny packets that match this rule.	option	-

Parameter	Description	Type	Size

	Option	Description	
	<i>permit</i>	Allow or permit packets that match this rule.	
	<i>deny</i>	Deny packets that match this rule.	

flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
ge	Minimum prefix length to be matched (0 - 128).	integer	Minimum value: 0 Maximum value: 128
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
le	Maximum prefix length to be matched (0 - 128).	integer	Minimum value: 0 Maximum value: 128
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified

config router rip

Configure RIP.

```
config router rip
  Description: Configure RIP.
  set default-information-originate [enable|disable]
  set default-metric {integer}
  config distance
    Description: distance
    edit <id>
      set access-list {string}
      set distance {integer}
      set prefix {ipv4-classnet-any}
    next
  end
  config distribute-list
    Description: Distribute list.
    edit <id>
      set direction [in|out]
```

```

        set interface {string}
        set listname {string}
        set status [enable|disable]
    next
end
set garbage-timer {integer}
config interface
    Description: RIP interface configuration.
    edit <name>
        set auth-keychain {string}
        set auth-mode [none|text|...]
        set auth-string {password}
        set flags {integer}
        set receive-version {option1}, {option2}, ...
        set send-version {option1}, {option2}, ...
        set send-version2-broadcast [disable|enable]
        set split-horizon [poisoned|regular]
        set split-horizon-status [enable|disable]
    next
end
set max-out-metric {integer}
config neighbor
    Description: neighbor
    edit <id>
        set ip {ipv4-address}
    next
end
config network
    Description: network
    edit <id>
        set prefix {ipv4-classnet}
    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set access-list {string}
        set direction [in|out]
        set interface {string}
        set offset {integer}
        set status [enable|disable]
    next
end
set passive-interface <name1>, <name2>, ...
set recv-buffer-size {integer}
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set routemap {string}
        set status [enable|disable]
    next
end
set timeout-timer {integer}
set update-timer {integer}
set version [1|2]

```

end

config router rip

Parameter	Description	Type	Size						
default-information-originate	Enable/disable generation of default route.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16						
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647						
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						
recv-buffer-size	Receiving buffer size.	integer	Minimum value: 8129 Maximum value: 2147483647						
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647						

Parameter	Description	Type	Size
update-timer	Update 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
access-list	Access list for route destination.	string	Maximum length: 35
distance	Distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255
id	Distance ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix	Distance prefix.	ipv4-classnet-any	Not Specified

config distribute-list

Parameter	Description	Type	Size
direction	Distribute list direction.	option	-
	Option	Description	
	<i>in</i>	Filter incoming packets.	
	<i>out</i>	Filter outgoing packets.	

Parameter	Description	Type	Size
id	Distribute list ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Distribute list interface name.	string	Maximum length: 15
listname	Distribute access/prefix list name.	string	Maximum length: 35
status	status	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	

config interface

Parameter	Description	Type	Size								
auth-keychain	Authentication key-chain name.	string	Maximum length: 35								
auth-mode	Authentication mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>md5</i></td><td>MD5.</td></tr></table>			Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>md5</i>	MD5.
	Option	Description									
	<i>none</i>	None.									
	<i>text</i>	Text.									
<i>md5</i>	MD5.										
auth-string	Authentication string/password.	password	Not Specified								
flags	flags Read-only.	integer	Minimum value: 0 Maximum value: 255								
name	Interface name.	string	Maximum length: 35								
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	
	<i>disable</i>	Disable broadcasting.	
	<i>enable</i>	Enable broadcasting.	
split-horizon	Enable/disable split horizon.	option	-
	Option	Description	
	<i>poisoned</i>	Poisoned.	
	<i>regular</i>	Regular.	
split-horizon-status	Enable/disable split horizon.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config neighbor

Parameter	Description	Type	Size
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IP address.	ipv4-address	Not Specified

config network

Parameter	Description	Type	Size
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix	Network prefix.	ipv4-classnet	Not Specified

config offset-list

Parameter	Description	Type	Size
access-list	Access list name.	string	Maximum length: 35
direction	Offset list direction.	option	-
	Option	Description	
	in	Filter incoming packets.	
	out	Filter outgoing packets.	
id	Offset-list ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Interface name.	string	Maximum length: 15
offset	offset	integer	Minimum value: 1 Maximum value: 16
status	status	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	

config redistribute

Parameter	Description	Type	Size
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16
name	Redistribute name.	string	Maximum length: 35
route-map	Route map name.	string	Maximum length: 35
status	status	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config router ripng

Configure RIPng.

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

```

set garbage-timer {integer}
config interface
    Description: RIPng interface configuration.
    edit <name>
        set flags {integer}
        set split-horizon [poisoned|regular]
        set split-horizon-status [enable|disable]
    next
end
set max-out-metric {integer}
config neighbor
    Description: neighbor
    edit <id>
        set interface {string}
        set ip6 {ipv6-address}
    next
end
config network
    Description: Network.
    edit <id>
        set prefix {ipv6-prefix}
    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set access-list6 {string}
        set direction [in|out]
        set interface {string}
        set offset {integer}
        set status [enable|disable]
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration. Read-only.
    edit <name>
        set metric {integer}
        set routemap {string}
        set status [enable|disable]
    next
end
set timeout-timer {integer}
set update-timer {integer}
end

```

config router ripng

Parameter	Description	Type	Size
default-information-originate	Enable/disable generation of default route.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16
garbage-timer	Garbage timer.	integer	Minimum value: 5 Maximum value: 2147483647
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
timeout-timer	Timeout timer.	integer	Minimum value: 5 Maximum value: 2147483647
update-timer	Update timer.	integer	Minimum value: 5 Maximum value: 2147483647

config aggregate-address

Parameter	Description	Type	Size
id	Aggregate address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	Aggregate address prefix.	ipv6-prefix	Not Specified

config distance

Parameter	Description	Type	Size
access-list6	Access list for route destination.	string	Maximum length: 35
distance	Distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255
id	Distance ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix6	Distance prefix6.	ipv6-prefix	Not Specified

config distribute-list

Parameter	Description	Type	Size						
direction	Distribute list direction.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></table>	Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.		
	Option	Description							
	<i>in</i>	Filter incoming packets.							
<i>out</i>	Filter outgoing packets.								
id	Distribute list ID.	integer	Minimum value: 0 Maximum value: 4294967295						
interface	Distribute list interface name.	string	Maximum length: 15						
listname	Distribute access/prefix list name.	string	Maximum length: 35						
status	status	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								

config interface

Parameter	Description	Type	Size
flags	Flags. Read-only.	integer	Minimum value: 0 Maximum value: 255
name	Interface name.	string	Maximum length: 35
split-horizon	Enable/disable split horizon.	option	-
	Option		Description
	<i>poisoned</i>		Poisoned.
	<i>regular</i>		Regular.
split-horizon-status	Enable/disable split horizon.	option	-
	Option		Description
	<i>enable</i>		Enable setting.
	<i>disable</i>		Disable setting.

config neighbor

Parameter	Description	Type	Size
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Interface name.	string	Maximum length: 15
ip6	IPv6 link-local address.	ipv6-address	Not Specified

config network

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

Parameter	Description	Type	Size
prefix	Network IPv6 link-local prefix.	ipv6-prefix	Not Specified

config offset-list

Parameter	Description	Type	Size						
access-list6	IPv6 access list name.	string	Maximum length: 35						
direction	Offset list direction.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></table>			Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.
	Option	Description							
	<i>in</i>	Filter incoming packets.							
<i>out</i>	Filter outgoing packets.								
id	Offset-list ID.	integer	Minimum value: 0 Maximum value: 4294967295						
interface	Interface name.	string	Maximum length: 15						
offset	offset	integer	Minimum value: 1 Maximum value: 16						
status	status	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								

config redistribute

Parameter	Description	Type	Size
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16
name	Redistribute name.	string	Maximum length: 35

Parameter	Description	Type	Size
route-map	Route map name.	string	Maximum length: 35
status	status	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config router route-map

Configure route maps.

```

config router route-map
  Description: Configure route maps.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set match-as-path {string}
        set match-community {string}
        set match-community-exact [enable|disable]
        set match-flags {integer}
        set match-interface {string}
        set match-ip-address {string}
        set match-ip-nexthop {string}
        set match-ip6-address {string}
        set match-ip6-nexthop {string}
        set match-metric {integer}
        set match-origin [none|egp|...]
        set match-route-type [1|2|...]
        set match-tag {integer}
        set set-aggregator-as {integer}
        set set-aggregator-ip {ipv4-address-any}
        set set-aspath <as1>, <as2>, ...
        set set-aspath-action [prepend|replace]
        set set-atomic-aggregate [enable|disable]
        set set-community <community1>, <community2>, ...
        set set-community-additive [enable|disable]
        set set-community-delete {string}
        set set-dampening-max-suppress {integer}
        set set-dampening-reachability-half-life {integer}
        set set-dampening-reuse {integer}
        set set-dampening-suppress {integer}
        set set-dampening-unreachability-half-life {integer}
        set set-extcommunity-rt <community1>, <community2>, ...
        set set-extcommunity-soo <community1>, <community2>, ...
        set set-flags {integer}

```

```

        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-origin [none|egp|...]
        set set-originator-id {ipv4-address-any}
        set set-route-tag {integer}
        set set-tag {integer}
        set set-weight {integer}
    next
end
next
end

```

config router route-map

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

config rule

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>permit</i>	Permit.	
	<i>deny</i>	Deny.	
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
match-as-path	Match BGP AS path list.	string	Maximum length: 35
match-community	Match BGP community list.	string	Maximum length: 35
match-community-exact	Enable/disable exact matching of communities.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exact matching of communities.</td></tr><tr><td><i>disable</i></td><td>Disable exact matching of communities.</td></tr></table>	Option	Description	<i>enable</i>	Enable exact matching of communities.	<i>disable</i>	Disable exact matching of communities.						
	Option	Description											
	<i>enable</i>	Enable exact matching of communities.											
<i>disable</i>	Disable exact matching of communities.												
match-flags	BGP flag value to match (0 - 65535) Read-only.	integer	Minimum value: 0 Maximum value: 65535										
match-interface	Match interface configuration.	string	Maximum length: 15										
match-ip-address	Match IP address permitted by access-list or prefix-list.	string	Maximum length: 35										
match-ip-nexthop	Match next hop IP address passed by access-list or prefix-list.	string	Maximum length: 35										
match-ip6-address	Match IPv6 address permitted by access-list6 or prefix-list6.	string	Maximum length: 35										
match-ip6-nexthop	Match next hop IPv6 address passed by access-list6 or prefix-list6.	string	Maximum length: 35										
match-metric	Match metric for redistribute routes.	integer	Minimum value: 0 Maximum value: 4294967295										
match-origin	Match BGP origin code.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>egp</i></td><td>Remote EGP.</td></tr><tr><td><i>igp</i></td><td>Local IGP.</td></tr><tr><td><i>incomplete</i></td><td>Unknown heritage.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>egp</i>	Remote EGP.	<i>igp</i>	Local IGP.	<i>incomplete</i>	Unknown heritage.		
	Option	Description											
	<i>none</i>	None.											
	<i>egp</i>	Remote EGP.											
	<i>igp</i>	Local IGP.											
<i>incomplete</i>	Unknown heritage.												
match-route-type	Match route type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1</i></td><td>External type 1.</td></tr><tr><td><i>2</i></td><td>External type 2.</td></tr><tr><td><i>none</i></td><td>No type specified.</td></tr></table>	Option	Description	<i>1</i>	External type 1.	<i>2</i>	External type 2.	<i>none</i>	No type specified.				
	Option	Description											
	<i>1</i>	External type 1.											
	<i>2</i>	External type 2.											
<i>none</i>	No type specified.												

Parameter	Description	Type	Size
match-tag	Match tag.	integer	Minimum value: 0 Maximum value: 4294967295
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 <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-aspath-action	Specify preferred action of set-aspath.	option	-

Option	Description
<i>prepend</i>	Prepend.
<i>replace</i>	Replace.

set-atomic-aggregate	Enable/disable BGP atomic aggregate attribute.	option	-

Option	Description
<i>enable</i>	Enable BGP atomic aggregate attribute.
<i>disable</i>	Disable BGP atomic aggregate attribute.

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
<i>enable</i>	Enable adding set-community to existing community.
<i>disable</i>	Disable adding set-community to existing community.

set-community-delete	Delete communities matching community list.	string	Maximum length: 35

Parameter	Description	Type	Size
set-dampening-max-suppress	Maximum duration to suppress a route (1 - 255 min, 0 = unset).	integer	Minimum value: 0 Maximum value: 255
set-dampening-reachability-half-life	Reachability half-life time for the penalty (1 - 45 min, 0 = unset).	integer	Minimum value: 0 Maximum value: 45
set-dampening-reuse	Value to start reusing a route (1 - 20000, 0 = unset).	integer	Minimum value: 0 Maximum value: 20000
set-dampening-suppress	Value to start suppressing a route (1 - 20000, 0 = unset).	integer	Minimum value: 0 Maximum value: 20000
set-dampening-unreachability-half-life	Unreachability Half-life time for the penalty (1 - 45 min, 0 = unset)	integer	Minimum value: 0 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-flags	BGP flags value (0 - 65535) Read-only.	integer	Minimum value: 0 Maximum value: 65535
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

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

config router setting

Configure router settings.


```

config router setting
    Description: Configure router settings.
    set hostname {string}
    set show-filter {string}
end

```

config router setting

Parameter	Description	Type	Size
hostname	Hostname for this virtual domain router.	string	Maximum length: 14
show-filter	Prefix-list as filter for showing routes.	string	Maximum length: 35

config router static

Configure IPv4 static routing tables.

```

config router static
    Description: Configure IPv4 static routing tables.
    edit <seq-num>
        set bfd [enable|disable]
        set blackhole [enable|disable]
        set comment {var-string}
        set device {string}
        set distance {integer}
        set dst {ipv4-classnet}
        set dstaddr {string}
        set dynamic-gateway [enable|disable]
        set gateway {ipv4-address}
        set internet-service {integer}
        set internet-service-custom {string}
        set link-monitor-exempt [enable|disable]
        set priority {integer}
        set src {ipv4-classnet}
        set status [enable|disable]
        set virtual-wan-link [enable|disable]
        set vrf {integer}
        set weight {integer}
    next
end

```

config router static

Parameter	Description	Type	Size						
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).		
	Option	Description							
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).							
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).								
blackhole	Enable/disable black hole.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable black hole.</td></tr><tr><td><i>disable</i></td><td>Disable black hole.</td></tr></table>	Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.		
	Option	Description							
	<i>enable</i>	Enable black hole.							
<i>disable</i>	Disable black hole.								
comment	Optional comments.	var-string	Maximum length: 255						
device	Gateway out interface or tunnel.	string	Maximum length: 35						
distance	Administrative distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255						
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified						
dstaddr	Name of firewall address or address group.	string	Maximum length: 79						
dynamic-gateway	Enable use of dynamic gateway retrieved from a DHCP or PPP server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic gateway.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic gateway.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic gateway.	<i>disable</i>	Disable dynamic gateway.		
	Option	Description							
	<i>enable</i>	Enable dynamic gateway.							
<i>disable</i>	Disable dynamic gateway.								
gateway	Gateway IP for this route.	ipv4-address	Not Specified						
internet-service	Application ID in the Internet service database.	integer	Minimum value: 0 Maximum value: 4294967295						

Parameter	Description	Type	Size
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.	
	disable	Disable withdrawal of this static route when link monitor or health check is down.	
priority	Administrative priority (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295
src	Source prefix for this route.	ipv4-classnet	Not Specified
status	Enable/disable this static route.	option	-
	Option	Description	
	enable	Enable static route.	
	disable	Disable static route.	
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.	
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31
weight	Administrative weight (0 - 255).	integer	Minimum value: 0 Maximum value: 255

config router static6

Configure IPv6 static routing tables.

```
config router static6
  Description: Configure IPv6 static routing tables.
  edit <seq-num>
    set bfd [enable|disable]
    set blackhole [enable|disable]
    set comment {var-string}
    set device {string}
    set devindex {integer}
    set distance {integer}
    set dst {ipv6-network}
    set gateway {ipv6-address}
    set link-monitor-exempt [enable|disable]
    set priority {integer}
    set status [enable|disable]
    set virtual-wan-link [enable|disable]
  next
end
```

config router static6

Parameter	Description	Type	Size
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-
	Option	Description	
	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	
	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).	
blackhole	Enable/disable black hole.	option	-
	Option	Description	
	<i>enable</i>	Enable black hole.	
	<i>disable</i>	Disable black hole.	
comment	Optional comments.	var-string	Maximum length: 255
device	Gateway out interface or tunnel.	string	Maximum length: 35

Parameter	Description	Type	Size
devindex	Device index (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
distance	Administrative distance (1 - 255).	integer	Minimum value: 1 Maximum value: 255
dst	Destination IPv6 prefix.	ipv6-network	Not Specified
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-

Option	Description
<i>enable</i>	Enable withdrawal of this static route when link monitor or health check is down.
<i>disable</i>	Disable withdrawal of this static route when link monitor or health check is down.

priority	Administrative priority (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295
status	Enable/disable this static route.	option	-

Option	Description
<i>enable</i>	Enable static route.
<i>disable</i>	Disable static route.

virtual-wan-link	Enable/disable egress through the virtual-wan-link.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 742](#)

config ssh-filter profile

SSH filter profile.

```
config ssh-filter profile
  Description: SSH filter profile.
  edit <name>
    set block {option1}, {option2}, ...
    set default-command-log [enable|disable]
    config file-filter
      Description: File filter.
      config entries
        Description: File filter entries.
        edit <filter>
          set action [log|block]
          set comment {var-string}
          set direction [incoming|outgoing|...]
          set file-type <name1>, <name2>, ...
          set password-protected [yes|any]
        next
      end
    set log [enable|disable]
    set scan-archive-contents [enable|disable]
    set status [enable|disable]
  end
  set log {option1}, {option2}, ...
  config shell-commands
    Description: SSH command filter.
    edit <id>
      set action [block|allow]
      set alert [enable|disable]
      set log [enable|disable]
      set pattern {string}
      set severity [low|medium|...]
      set type [simple|regex]
    next
  end
next
end
```

config ssh-filter profile

Parameter	Description	Type	Size																		
block	SSH blocking options.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>x11</i></td><td>X server forwarding.</td></tr><tr><td><i>shell</i></td><td>SSH shell.</td></tr><tr><td><i>exec</i></td><td>SSH execution.</td></tr><tr><td><i>port-forward</i></td><td>Port forwarding.</td></tr><tr><td><i>tun-forward</i></td><td>Tunnel forwarding.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>scp</i></td><td>SCP.</td></tr><tr><td><i>unknown</i></td><td>Unknown channel.</td></tr></table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.		
Option	Description																				
<i>x11</i>	X server forwarding.																				
<i>shell</i>	SSH shell.																				
<i>exec</i>	SSH execution.																				
<i>port-forward</i>	Port forwarding.																				
<i>tun-forward</i>	Tunnel forwarding.																				
<i>sftp</i>	SFTP.																				
<i>scp</i>	SCP.																				
<i>unknown</i>	Unknown channel.																				
default-command-log	Enable/disable logging unmatched shell commands.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable log unmatched shell commands.</td></tr><tr><td><i>disable</i></td><td>Disable log unmatched shell commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable log unmatched shell commands.	<i>disable</i>	Disable log unmatched shell commands.														
Option	Description																				
<i>enable</i>	Enable log unmatched shell commands.																				
<i>disable</i>	Disable log unmatched shell commands.																				
log	SSH logging options.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>x11</i></td><td>X server forwarding.</td></tr><tr><td><i>shell</i></td><td>SSH shell.</td></tr><tr><td><i>exec</i></td><td>SSH execution.</td></tr><tr><td><i>port-forward</i></td><td>Port forwarding.</td></tr><tr><td><i>tun-forward</i></td><td>Tunnel forwarding.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>scp</i></td><td>SCP.</td></tr><tr><td><i>unknown</i></td><td>Unknown channel.</td></tr></table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.		
Option	Description																				
<i>x11</i>	X server forwarding.																				
<i>shell</i>	SSH shell.																				
<i>exec</i>	SSH execution.																				
<i>port-forward</i>	Port forwarding.																				
<i>tun-forward</i>	Tunnel forwarding.																				
<i>sftp</i>	SFTP.																				
<i>scp</i>	SCP.																				
<i>unknown</i>	Unknown channel.																				
name	SSH filter profile name.	string	Maximum length: 35																		

config file-filter

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

config entries

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

Parameter	Description	Type	Size
file-type <name>	Select file type. File type name.	string	Maximum length: 39
filter	Add a file filter.	string	Maximum length: 35
password-protected	Match password-protected files.	option	-
	Option	Description	
	yes	Match only password-protected files.	
	any	Match any file.	

config shell-commands

Parameter	Description	Type	Size						
action	Action to take for URL filter matches.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block the SSH shell command.</td></tr><tr><td><i>allow</i></td><td>Allow the SSH shell command.</td></tr></table>	Option	Description	<i>block</i>	Block the SSH shell command.	<i>allow</i>	Allow the SSH shell command.		
Option	Description								
<i>block</i>	Block the SSH shell command.								
<i>allow</i>	Allow the SSH shell command.								
alert	Enable/disable alert.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable alert.</td></tr><tr><td><i>disable</i></td><td>Disable alert.</td></tr></table>	Option	Description	<i>enable</i>	Enable alert.	<i>disable</i>	Disable alert.		
Option	Description								
<i>enable</i>	Enable alert.								
<i>disable</i>	Disable alert.								
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295						
log	Enable/disable logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.		
Option	Description								
<i>enable</i>	Enable logging.								
<i>disable</i>	Disable logging.								
pattern	SSH shell command pattern.	string	Maximum length: 128						

Parameter	Description	Type	Size
severity	Log severity.	option	-

Option	Description
<i>low</i>	Severity low.
<i>medium</i>	Severity medium.
<i>high</i>	Severity high.
<i>critical</i>	Severity critical.

type	Matching type.	option	-

Option	Description
<i>simple</i>	Match single command.
<i>regex</i>	Match command line using regular expression.

switch-controller

This section includes syntax for the following commands:

- [config switch-controller 802-1X-settings on page 748](#)
- [config switch-controller auto-config custom on page 749](#)
- [config switch-controller auto-config default on page 751](#)
- [config switch-controller auto-config policy on page 752](#)
- [config switch-controller custom-command on page 754](#)
- [config switch-controller flow-tracking on page 755](#)
- [config switch-controller global on page 758](#)
- [config switch-controller igmp-snooping on page 762](#)
- [config switch-controller lldp-profile on page 763](#)
- [config switch-controller lldp-settings on page 767](#)
- [config switch-controller location on page 768](#)
- [config switch-controller managed-switch on page 773](#)
- [config switch-controller network-monitor-settings on page 801](#)
- [config switch-controller qos dot1p-map on page 802](#)
- [config switch-controller qos ip-dscp-map on page 806](#)
- [config switch-controller qos qos-policy on page 809](#)
- [config switch-controller qos queue-policy on page 810](#)
- [config switch-controller quarantine on page 813](#)
- [config switch-controller remote-log on page 814](#)
- [config switch-controller security-policy 802-1X on page 817](#)
- [config switch-controller security-policy local-access on page 820](#)
- [config switch-controller sflow on page 822](#)
- [config switch-controller snmp-community on page 823](#)
- [config switch-controller snmp-sysinfo on page 826](#)
- [config switch-controller snmp-trap-threshold on page 827](#)
- [config switch-controller snmp-user on page 829](#)
- [config switch-controller storm-control-policy on page 832](#)
- [config switch-controller storm-control on page 831](#)
- [config switch-controller stp-instance on page 834](#)
- [config switch-controller stp-settings on page 835](#)
- [config switch-controller switch-group on page 837](#)
- [config switch-controller switch-interface-tag on page 838](#)
- [config switch-controller switch-log on page 839](#)
- [config switch-controller switch-profile on page 840](#)
- [config switch-controller system on page 842](#)
- [config switch-controller traffic-policy on page 843](#)

- [config switch-controller traffic-sniffer on page 845](#)
- [config switch-controller virtual-port-pool on page 847](#)

config switch-controller 802-1X-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure global 802.1X settings.

```
config switch-controller 802-1X-settings
    Description: Configure global 802.1X settings.
    set link-down-auth [set-unauth|no-action]
    set max-reauth-attempt {integer}
    set reauth-period {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	-

Parameter	Description	Type	Size
	Option	Description	
	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.	
	<i>no-action</i>	Interface reauthentication is not needed.	
max-reauth-attempt	Maximum number of authentication attempts (0 - 15, default = 3).	integer	Minimum value: 0 Maximum value: 15
reauth-period	Period of time to allow for reauthentication (1 - 1440 sec, default = 60, 0 = disable reauthentication).	integer	Minimum value: 0 Maximum value: 1440

config switch-controller auto-config custom



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Policies which can override the 'default' for specific ISL/ICL/FortiLink interface.

```
config switch-controller auto-config custom
```

Description: Policies which can override the 'default' for specific ISL/ICL/FortiLink interface.

```
edit <name>
  config switch-binding
    Description: Switch binding list.
    edit <switch-id>
      set policy {string}
    next
  end
next
end
```

config switch-controller auto-config custom

Parameter	Description	Type	Size
name	Auto-Config FortiLink or ISL/ICL interface name.	string	Maximum length: 15

config switch-binding

Parameter	Description	Type	Size
policy	Custom auto-config policy.	string	Maximum length: 63
switch-id	Switch name.	string	Maximum length: 16

config switch-controller auto-config default



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.

```
config switch-controller auto-config default
    Description: Policies which are applied automatically to all ISL/ICL/FortiLink
interfaces.
    set fgt-policy {string}
    set icl-policy {string}
    set isl-policy {string}
end
```

config switch-controller auto-config default

Parameter	Description	Type	Size
fgt-policy	Default FortiLink auto-config policy.	string	Maximum length: 63
icl-policy	Default ICL auto-config policy.	string	Maximum length: 63
isl-policy	Default ISL auto-config policy.	string	Maximum length: 63

config switch-controller auto-config policy



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Policy definitions which can define the behavior on auto configured interfaces.

```
config switch-controller auto-config policy
    Description: Policy definitions which can define the behavior on auto configured
    interfaces.
    edit <name>
        set igmp-flood-report [enable|disable]
        set igmp-flood-traffic [enable|disable]
        set poe-status [enable|disable]
        set qos-policy {string}
        set storm-control-policy {string}
    next
end
```

config switch-controller auto-config policy

Parameter	Description	Type	Size
igmp-flood-report	Enable/disable IGMP flood report.	option	-

Parameter	Description	Type	Size
	Option	Description	
	enable	Enable IGMP flood report.	
	disable	Disable IGMP flood report.	
igmp-flood-traffic	Enable/disable IGMP flood traffic.	option	-
	Option	Description	
	enable	Enable IGMP flood traffic.	
	disable	Disable IGMP flood traffic.	
name	Auto-Config policy name	string	Maximum length: 63
poe-status	Enable/disable PoE status.	option	-
	Option	Description	
	enable	Enable PoE status.	
	disable	Disable PoE status.	
qos-policy	Auto-Config QoS policy.	string	Maximum length: 63
storm-control-policy	Auto-Config storm control policy.	string	Maximum length: 63

config switch-controller custom-command



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices.

```
config switch-controller custom-command
    Description: Configure the FortiGate switch controller to send custom commands to
managed FortiSwitch devices.
    edit <command-name>
        set command {var-string}
        set description {string}
    next
end
```

config switch-controller custom-command

Parameter	Description	Type	Size
command	String of commands to send to FortiSwitch devices (For example (%0a = return key): config switch trunk %0a edit myTrunk %0a set members port1 port2 %0a end %0a).	var-string	Maximum length: 4095
command-name	Command name called by the FortiGate switch controller in the execute command.	string	Maximum length: 35
description	Description.	string	Maximum length: 35

config switch-controller flow-tracking



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch flow tracking and export via ipfix/netflow.

```
config switch-controller flow-tracking
    Description: Configure FortiSwitch flow tracking and export via ipfix/netflow.
    config aggregates
        Description: Configure aggregates in which all traffic sessions matching the IP
        Address will be grouped into the same flow.
        edit <id>
            set ip {ipv4-classnet}
        next
    end
    set collector-ip {ipv4-address}
    set collector-port {integer}
    set format [netflow1|netflow5|...]
    set level [vlan|ip|...]
    set max-export-pkt-size {integer}
    set sample-mode [local|perimeter|...]
    set sample-rate {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}
```

```

set transport [udp|tcp|...]
end

```

config switch-controller flow-tracking

Parameter	Description	Type	Size
collector-ip	Configure collector ip address.	ipv4-address	Not Specified
collector-port	Configure collector port number(0-65535, default=0).	integer	Minimum value: 0 Maximum value: 65535
format	Configure flow tracking protocol.	option	-
	Option	Description	
	netflow1	Netflow version 1 sampling.	
	netflow5	Netflow version 5 sampling.	
	netflow9	Netflow version 9 sampling.	
	ipfix	Ipfix sampling.	
level	Configure flow tracking level.	option	-
	Option	Description	
	vlan	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.	
	ip	Collects srcip/dstip from the sample packet.	
	port	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.	
	proto	Collects srcip/dstip/protocol from the sample packet.	
	mac	Collects smac/dmac from the sample packet.	
max-export-pkt-size	Configure flow max export packet size (512-9216, default=512 bytes).	integer	Minimum value: 512 Maximum value: 9216
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.	

Parameter	Description	Type	Size
sample-rate	Configure sample rate for the perimeter and device-ingress sampling(0 - 99999).	integer	Minimum value: 0 Maximum value: 99999
timeout-general	Configure flow session general timeout (60-604800, default=3600 seconds).	integer	Minimum value: 60 Maximum value: 604800
timeout-icmp	Configure flow session ICMP timeout (60-604800, default=300 seconds).	integer	Minimum value: 60 Maximum value: 604800
timeout-max	Configure flow session max timeout (60-604800, default=604800 seconds).	integer	Minimum value: 60 Maximum value: 604800
timeout-tcp	Configure flow session TCP timeout (60-604800, default=3600 seconds).	integer	Minimum value: 60 Maximum value: 604800
timeout-tcp-fin	Configure flow session TCP FIN timeout (60-604800, default=300 seconds).	integer	Minimum value: 60 Maximum value: 604800
timeout-tcp-rst	Configure flow session TCP RST timeout (60-604800, default=120 seconds).	integer	Minimum value: 60 Maximum value: 604800
timeout-udp	Configure flow session UDP timeout (60-604800, default=300 seconds).	integer	Minimum value: 60 Maximum value: 604800
transport	Configure L4 transport protocol for exporting packets.	option	-

Option	Description
<i>udp</i>	UDP protocol.
<i>tcp</i>	TCP protocol.
<i>sctp</i>	SCTP protocol.

config aggregates

Parameter	Description	Type	Size
id	Aggregate id.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IP address to group all matching traffic sessions to a flow.	ipv4-classnet	Not Specified

config switch-controller global



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch global settings.

```
config switch-controller global
```

```
Description: Configure FortiSwitch global settings.
```

```
set allow-multiple-interfaces [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
set default-virtual-switch-vlan {string}
set disable-discovery <name1>, <name2>, ...
set https-image-push [enable|disable]
set log-mac-limit-violations [enable|disable]
set mac-aging-interval {integer}
set mac-event-logging [enable|disable]
set mac-retention-period {integer}
set mac-violation-timer {integer}
set sn-dns-resolution [enable|disable]
set vlan-all-mode [all|defined]
set vlan-optimization [enable|disable]
end

```

config switch-controller global

Parameter	Description	Type	Size						
allow-multiple-interfaces	Enable/disable multiple FortiLink interfaces for redundant connections between a managed FortiSwitch and FortiGate.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink on multiple interfaces.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink on multiple interfaces.</td></tr></table>			Option	Description	<i>enable</i>	Enable FortiLink on multiple interfaces.	<i>disable</i>	Disable FortiLink on multiple interfaces.
Option	Description								
<i>enable</i>	Enable FortiLink on multiple interfaces.								
<i>disable</i>	Disable FortiLink on multiple interfaces.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr><tr><td><i>enable</i></td><td>Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr></table>			Option	Description	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.
Option	Description								
<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.								
<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.								
default-virtual-switch-vlan	Default VLAN for ports when added to the virtual-switch.	string	Maximum length: 15						
disable-discovery <name>	Prevent this FortiSwitch from discovering. Managed device ID.	string	Maximum length: 79						
https-image-push	Enable/disable image push to FortiSwitch using HTTPS.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable image push to FortiSwitch using HTTPS.	
	<i>disable</i>	Disable image push to FortiSwitch using HTTPS.	
log-mac-limit-violations	Enable/disable logs for Learning Limit Violations.	option	-
	Option	Description	
	<i>enable</i>	Enable Learn Limit Violation.	
	<i>disable</i>	Disable Learn Limit Violation.	
mac-aging-interval	Time after which an inactive MAC is aged out (10 - 1000000 sec, default = 300, 0 = disable).	integer	Minimum value: 10 Maximum value: 1000000
mac-event-logging	Enable/disable MAC address event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable MAC address event logging.	
	<i>disable</i>	Disable MAC address event logging.	
mac-retention-period	Time in hours after which an inactive MAC is removed from client DB (0 = aged out based on mac-aging-interval).	integer	Minimum value: 0 Maximum value: 168
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	
	<i>enable</i>	Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	
	<i>disable</i>	Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	

Parameter	Description	Type	Size
vlan-all-mode	VLAN configuration mode, user-defined-vlans or all-possible-vlans.	option	-

Option	Description
<i>all</i>	Include all possible VLANs (1-4093).
<i>defined</i>	Include user defined VLANs.

vlan-optimization	FortiLink VLAN optimization.	option	-

Option	Description
<i>enable</i>	Enable VLAN optimization on FortiSwitch units for auto-generated trunks.
<i>disable</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.

config custom-command

Parameter	Description	Type	Size
command-entry	List of FortiSwitch commands.	string	Maximum length: 35
command-name	Name of custom command to push to all FortiSwitches in VDOM.	string	Maximum length: 35

config switch-controller igmp-snooping



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch IGMP snooping global settings.

```
config switch-controller igmp-snooping
    Description: Configure FortiSwitch IGMP snooping global settings.
    set aging-time {integer}
    set flood-unknown-multicast [enable|disable]
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 (15 - 3600 sec, default = 300).	integer	Minimum value: 15 Maximum value: 3600
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable unknown multicast flooding.	
	<i>disable</i>	Disable unknown multicast flooding.	

config switch-controller lldp-profile



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch LLDP profiles.

```
config switch-controller lldp-profile
  Description: Configure FortiSwitch LLDP profiles.
  edit <name>
    set 802 1-tlvs {option1}, {option2}, ...
    set 802 3-tlvs {option1}, {option2}, ...
    set auto-isl [disable|enable]
    set auto-isl-hello-timer {integer}
    set auto-isl-port-group {integer}
    set auto-isl-receive-timeout {integer}
    config custom-tlvs
      Description: Configuration method to edit custom TLV entries.
      edit <name>
        set information-string {user}
```

```

        set oui {user}
        set subtype {integer}
    next
end
config med-location-service
    Description: Configuration method to edit Media Endpoint Discovery (MED)
location service type-length-value (TLV) categories.
    edit <name>
        set status [disable|enable]
        set sys-location-id {string}
    next
end
config med-network-policy
    Description: Configuration method to edit Media Endpoint Discovery (MED) network
policy type-length-value (TLV) categories.
    edit <name>
        set assign-vlan [disable|enable]
        set dscp {integer}
        set priority {integer}
        set status [disable|enable]
        set vlan-intf {string}
    next
end
set med-tlvs {option1}, {option2}, ...
next
end

```

config switch-controller lldp-profile

Parameter	Description	Type	Size
802 1-tlvs	Transmitted IEEE 802.1 TLVs.	option	-
	Option	Description	
	<i>port-vlan-id</i>	Port native VLAN TLV.	
802 3-tlvs	Transmitted IEEE 802.3 TLVs.	option	-
	Option	Description	
	<i>max-frame-size</i>	Maximum frame size TLV.	
	<i>power-negotiation</i>	PoE+ classification TLV.	
auto-isf	Enable/disable auto inter-switch LAG.	option	-
	Option	Description	
	<i>disable</i>	Disable auto inter-switch-LAG.	
	<i>enable</i>	Enable auto inter-switch-LAG.	

Parameter	Description	Type	Size
auto-isl-hello-timer	Auto inter-switch LAG hello timer duration (1 - 30 sec, default = 3).	integer	Minimum value: 1 Maximum value: 30
auto-isl-port-group	Auto inter-switch LAG port group ID (0 - 9).	integer	Minimum value: 0 Maximum value: 9
auto-isl-receive-timeout	Auto inter-switch LAG timeout if no response is received (3 - 90 sec, default = 9).	integer	Minimum value: 0 Maximum value: 90
med-tlvs	Transmitted LLDP-MED TLVs (type-length-value descriptions).	option	-

Option	Description
<i>inventory-management</i>	Inventory management TLVs.
<i>network-policy</i>	Network policy TLVs.
<i>power-management</i>	Power management TLVs.
<i>location-identification</i>	Location identification TLVs.

name	Profile name.	string	Maximum length: 63

config custom-tlvs

Parameter	Description	Type	Size
information-string	Organizationally defined information string (0 - 507 hexadecimal bytes).	user	Not Specified
name	TLV name (not sent).	string	Maximum length: 63
oui	Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.	user	Not Specified
subtype	Organizationally defined subtype (0 - 255).	integer	Minimum value: 0 Maximum value: 255

config med-location-service

Parameter	Description	Type	Size
name	Location service type name.	string	Maximum length: 63
status	Enable or disable this TLV.	option	-
	Option	Description	
	<i>disable</i>	Do not transmit this location service TLV.	
	<i>enable</i>	Transmit this location service TLV.	
sys-location-id	Location service ID.	string	Maximum length: 63

config med-network-policy

Parameter	Description	Type	Size
assign-vlan	Enable/disable VLAN assignment when this profile is applied on managed FortiSwitch port.	option	-
	Option	Description	
	<i>disable</i>	Disable VLAN assignment when this profile is applied on port.	
	<i>enable</i>	Enable VLAN assignment when this profile is applied on port.	
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
name	Policy type name.	string	Maximum length: 63
priority	Advertised Layer 2 priority (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
status	Enable or disable this TLV.	option	-
	Option	Description	
	<i>disable</i>	Do not transmit this network policy TLV.	
	<i>enable</i>	Transmit this TLV if a VLAN has been added to the port.	
vlan-intf	VLAN interface to advertise; if configured on port.	string	Maximum length: 15

config switch-controller lldp-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch LLDP settings.

```
config switch-controller lldp-settings
    Description: Configure FortiSwitch LLDP settings.
    set fast-start-interval {integer}
    set management-interface [internal|mgmt]
    set tx-hold {integer}
    set tx-interval {integer}
end
```

config switch-controller lldp-settings

Parameter	Description	Type	Size
fast-start-interval	Frequency of LLDP PDU transmission from FortiSwitch for the first 4 packets when the link is up (2 - 5 sec, default = 2, 0 = disable fast start).	integer	Minimum value: 0 Maximum value: 255
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>internal</i>	Use internal interface.	
	<i>mgmt</i>	Use management interface.	
tx-hold	Number of tx-intervals before local LLDP data expires (1 - 16, default = 4). Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 1 Maximum value: 16
tx-interval	Frequency of LLDP PDU transmission from FortiSwitch (5 - 4095 sec, default = 30). Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 5 Maximum value: 4095

config switch-controller location



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch location services.

```
config switch-controller location
    Description: Configure FortiSwitch location services.
    edit <name>
```



```

config address-civic
    Description: Configure location civic address.
    set additional {string}
    set additional-code {string}
    set block {string}
    set branch-road {string}
    set building {string}
    set city {string}
    set city-division {string}
    set country {string}
    set country-subdivision {string}
    set county {string}
    set direction {string}
    set floor {string}
    set landmark {string}
    set language {string}
    set name {string}
    set number {string}
    set number-suffix {string}
    set parent-key {string}
    set place-type {string}
    set post-office-box {string}
    set postal-community {string}
    set primary-road {string}
    set road-section {string}
    set room {string}
    set script {string}
    set seat {string}
    set street {string}
    set street-name-post-mod {string}
    set street-name-pre-mod {string}
    set street-suffix {string}
    set sub-branch-road {string}
    set trailing-str-suffix {string}
    set unit {string}
    set zip {string}
end
config coordinates
    Description: Configure location GPS coordinates.
    set altitude {string}
    set altitude-unit [m|f]
    set datum [WGS84|NAD83|...]
    set latitude {string}
    set longitude {string}
    set parent-key {string}
end
config elin-number
    Description: Configure location ELIN number.
    set elin-num {string}
    set parent-key {string}
end
next
end

```

config switch-controller location

Parameter	Description	Type	Size
name	Unique location item name.	string	Maximum length: 63

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
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

Parameter	Description	Type	Size
number	House number.	string	Maximum length: 47
number-suffix	House number suffix.	string	Maximum length: 47
parent-key	Parent key name. Read-only.	string	Maximum length: 63
place-type	Placetype.	string	Maximum length: 47
post-office-box	Post office box (P.O. box).	string	Maximum length: 47
postal-community	Postal community name.	string	Maximum length: 47
primary-road	Primary road name.	string	Maximum length: 47
road-section	Road section.	string	Maximum length: 47
room	Room number.	string	Maximum length: 47
script	Script used to present the address information.	string	Maximum length: 47
seat	Seat number.	string	Maximum length: 47
street	Street.	string	Maximum length: 47
street-name-post-mod	Street name post modifier.	string	Maximum length: 47
street-name-pre-mod	Street name pre modifier.	string	Maximum length: 47
street-suffix	Street suffix.	string	Maximum length: 47
sub-branch-road	Sub branch road name.	string	Maximum length: 47
trailing-str-suffix	Trailing street suffix.	string	Maximum length: 47
unit	Unit (apartment, suite).	string	Maximum length: 47
zip	Postal/zip code.	string	Maximum length: 47

config coordinates

Parameter	Description	Type	Size
altitude	+/- Floating point no. eg. 117.47.	string	Maximum length: 15
altitude-unit	m (meters), f (floors).	option	-
	Option	Description	
	<i>m</i>	set altitude unit meters	
	<i>f</i>	set altitude unit floors	
datum	WGS84, NAD83, NAD83/MLLW.	option	-
	Option	Description	
	<i>WGS84</i>	set coordinates datum WGS84	
	<i>NAD83</i>	set coordinates datum NAD83	
	<i>NAD83/MLLW</i>	set coordinates datum NAD83/MLLW	
latitude	Floating point start with (+/-) or end with (N or S) eg. +/-16.67 or 16.67N.	string	Maximum length: 15
longitude	Floating point start with (+/-) or end with (E or W) eg. +/-26.789 or 26.789E.	string	Maximum length: 15
parent-key	Parent key name. Read-only.	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. Read-only.	string	Maximum length: 63

config switch-controller managed-switch



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch devices that are managed by this FortiGate.

```
config switch-controller managed-switch
  Description: Configure FortiSwitch devices that are managed by this FortiGate.
  edit <switch-id>
    config 802-1X-settings
      Description: Configuration method to edit FortiSwitch 802.1X global settings.
      set link-down-auth [set-unauth|no-action]
      set local-override [enable|disable]
      set max-reauth-attempt {integer}
      set reauth-period {integer}
    end
    set access-profile {string}
    config custom-command
      Description: Configuration method to edit FortiSwitch commands to be pushed to
this FortiSwitch device upon rebooting the FortiGate switch controller or the FortiSwitch.
      edit <command-entry>
        set command-name {string}
      next
    end
    set delayed-restart-trigger {integer}
    set description {string}
    set directly-connected {integer}
    set dynamic-capability {integer}
    set dynamically-discovered {integer}
```

```

set flow-identity {user}
set fsw-wan1-admin [discovered|disable|...]
set fsw-wan1-peer {string}
config igmp-snooping
    Description: Configure FortiSwitch IGMP snooping global settings.
    set aging-time {integer}
    set flood-unknown-multicast [enable|disable]
    set local-override [enable|disable]
end
set mclag-igmp-snooping-aware [enable|disable]
config mirror
    Description: Configuration method to edit FortiSwitch packet mirror.
    edit <name>
        set dst {string}
        set src-egress <name1>, <name2>, ...
        set src-ingress <name1>, <name2>, ...
        set status [active|inactive]
        set switching-packet [enable|disable]
    next
end
set name {string}
set override-snmp-community [enable|disable]
set override-snmp-sysinfo [disable|enable]
set override-snmp-trap-threshold [enable|disable]
set override-snmp-user [enable|disable]
set owner-vdom {string}
set poe-detection-type {integer}
set poe-lldp-detection [enable|disable]
set poe-pre-standard-detection [enable|disable]
config ports
    Description: Managed-switch port list.
    edit <port-name>
        set allowed-vlans <vlan-name1>, <vlan-name2>, ...
        set allowed-vlans-all [enable|disable]
        set arp-inspection-trust [untrusted|trusted]
        set bundle [enable|disable]
        set description {string}
        set dhcp-snoop-option82-trust [enable|disable]
        set dhcp-snooping [untrusted|trusted]
        set discard-mode [none|all-untagged|...]
        set edge-port [enable|disable]
        set export-tags <tag-name1>, <tag-name2>, ...
        set export-to {string}
        set export-to-pool {string}
        set fgt-peer-device-name {string}
        set fgt-peer-port-name {string}
        set fiber-port {integer}
        set flags {integer}
        set fortilink-port {integer}
        set igmp-snooping [enable|disable]
        set igmps-flood-reports [enable|disable]
        set igmps-flood-traffic [enable|disable]
        set isl-local-trunk-name {string}
        set isl-peer-device-name {string}
        set isl-peer-port-name {string}
        set lacp-speed [slow|fast]
    
```

```

        set learning-limit {integer}
        set lldp-profile {string}
        set lldp-status [disable|rx-only|...]
        set loop-guard [enabled|disabled]
        set loop-guard-timeout {integer}
        set mac-addr {mac-address}
        set max-bundle {integer}
        set mclag [enable|disable]
        set member-withdrawal-behavior [forward|block]
        set members <member-name1>, <member-name2>, ...
        set min-bundle {integer}
        set mode [static|lacp-passive|...]
        set packet-sample-rate {integer}
        set packet-sampler [enabled|disabled]
        set poe-capable {integer}
        set poe-pre-standard-detection [enable|disable]
        set poe-status [enable|disable]
        set port-number {integer}
        set port-owner {string}
        set port-prefix-type {integer}
        set port-security-policy {string}
        set port-selection-criteria [src-mac|dst-mac|...]
        set qos-policy {string}
        set sample-direction [tx|rx|...]
        set sflow-counter-interval {integer}
        set speed [10half|10full|...]
        set stacking-port {integer}
        set status [up|down]
        set sticky-mac [enable|disable]
        set storm-control-policy {string}
        set stp-bpdu-guard [enabled|disabled]
        set stp-bpdu-guard-timeout {integer}
        set stp-root-guard [enabled|disabled]
        set stp-state [enabled|disabled]
        set switch-id {string}
        set type [physical|trunk]
        set untagged-vlans <vlan-name1>, <vlan-name2>, ...
        set vlan {string}
    next
end
set pre-provisioned {integer}
config remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
    edit <name>
        set csv [enable|disable]
        set facility [kernel|user|...]
        set port {integer}
        set server {string}
        set severity [emergency|alert|...]
        set status [enable|disable]
    next
end
config snmp-community
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) communities.
    edit <id>

```

```

        set events {option1}, {option2}, ...
    config hosts
        Description: Configure IPv4 SNMP managers (hosts).
        edit <id>
            set ip {user}
        next
    end
    set name {string}
    set query-v1-port {integer}
    set query-v1-status [disable|enable]
    set query-v2c-port {integer}
    set query-v2c-status [disable|enable]
    set status [disable|enable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v1-status [disable|enable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set trap-v2c-status [disable|enable]
next
end
config snmp-sysinfo
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) system info.
    set contact-info {string}
    set description {string}
    set engine-id {string}
    set location {string}
    set status [disable|enable]
end
config snmp-trap-threshold
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) trap threshold values.
    set trap-high-cpu-threshold {integer}
    set trap-log-full-threshold {integer}
    set trap-low-memory-threshold {integer}
end
config snmp-user
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) users.
    edit <name>
        set auth-proto [md5|sha]
        set auth-pwd {password}
        set priv-proto [aes|des]
        set priv-pwd {password}
        set queries [disable|enable]
        set query-port {integer}
        set security-level [no-auth-no-priv|auth-no-priv|...]
    next
end
set staged-image-version {string}
config static-mac
    Description: Configuration method to edit FortiSwitch Static and Sticky MAC.
    edit <id>
        set description {string}
        set interface {string}

```



```

        set mac {mac-address}
        set type [static|sticky]
        set vlan {string}
    next
end
config storm-control
    Description: Configuration method to edit FortiSwitch storm control for
measuring traffic activity using data rates to prevent traffic disruption.
    set broadcast [enable|disable]
    set local-override [enable|disable]
    set rate {integer}
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
end
config stp-instance
    Description: Configuration method to edit Spanning Tree Protocol (STP)
instances.
    edit <id>
        set priority [0|4096|...]
    next
end
config stp-settings
    Description: Configuration method to edit Spanning Tree Protocol (STP) settings
used to prevent bridge loops.
    set forward-time {integer}
    set hello-time {integer}
    set local-override [enable|disable]
    set max-age {integer}
    set max-hops {integer}
    set name {string}
    set pending-timer {integer}
    set revision {integer}
end
set switch-device-tag {string}
config switch-log
    Description: Configuration method to edit FortiSwitch logging settings (logs are
transferred to and inserted into the FortiGate event log).
    set local-override [enable|disable]
    set severity [emergency|alert|...]
    set status [enable|disable]
end
set switch-profile {string}
set type [virtual|physical]
set version {integer}
next
end

```

config switch-controller managed-switch

Parameter	Description	Type	Size
access-profile	FortiSwitch access profile.	string	Maximum length: 31

Parameter	Description	Type	Size								
delayed-restart-trigger	Delayed restart triggered for this FortiSwitch.	integer	Minimum value: 0 Maximum value: 255								
description	Description.	string	Maximum length: 63								
directly-connected	Directly connected FortiSwitch. Read-only.	integer	Minimum value: 0 Maximum value: 1								
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								
dynamically-discovered	Dynamically discovered FortiSwitch. Read-only.	integer	Minimum value: 0 Maximum value: 1								
flow-identity	Flow-tracking netflow ipfix switch identity in hex format(00000000-FFFFFFFF default=0).	user	Not Specified								
fsw-wan1-admin	FortiSwitch WAN1 admin status; enable to authorize the FortiSwitch as a managed switch.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>discovered</td><td>Link waiting to be authorized.</td></tr><tr><td>disable</td><td>Link unauthorized.</td></tr><tr><td>enable</td><td>Link authorized.</td></tr></table>			Option	Description	discovered	Link waiting to be authorized.	disable	Link unauthorized.	enable	Link authorized.
	Option	Description									
	discovered	Link waiting to be authorized.									
	disable	Link unauthorized.									
enable	Link authorized.										
fsw-wan1-peer	Fortiswitch WAN1 peer port.	string	Maximum length: 35								
mclag-igmp-snooping-aware	Enable/disable MCLAG IGMP-snooping awareness.	option	-								

Option	Description
<i>enable</i>	Enable MCLAG IGMP-snooping awareness.
<i>disable</i>	Disable MCLAG IGMP-snooping awareness.

Parameter	Description	Type	Size						
name	Managed-switch name.	string	Maximum length: 35						
override-snmp-community	Enable/disable overriding the global SNMP communities.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global SNMP communities.</td></tr><tr><td><i>disable</i></td><td>Use the global SNMP communities.</td></tr></table>	Option	Description	<i>enable</i>	Override the global SNMP communities.	<i>disable</i>	Use the global SNMP communities.		
Option	Description								
<i>enable</i>	Override the global SNMP communities.								
<i>disable</i>	Use the global SNMP communities.								
override-snmp-sysinfo	Enable/disable overriding the global SNMP system information.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Use the global SNMP system information.</td></tr><tr><td><i>enable</i></td><td>Override the global SNMP system information.</td></tr></table>	Option	Description	<i>disable</i>	Use the global SNMP system information.	<i>enable</i>	Override the global SNMP system information.		
Option	Description								
<i>disable</i>	Use the global SNMP system information.								
<i>enable</i>	Override the global SNMP system information.								
override-snmp-trap-threshold	Enable/disable overriding the global SNMP trap threshold values.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global SNMP trap threshold values.</td></tr><tr><td><i>disable</i></td><td>Use the global SNMP trap threshold values.</td></tr></table>	Option	Description	<i>enable</i>	Override the global SNMP trap threshold values.	<i>disable</i>	Use the global SNMP trap threshold values.		
Option	Description								
<i>enable</i>	Override the global SNMP trap threshold values.								
<i>disable</i>	Use the global SNMP trap threshold values.								
override-snmp-user	Enable/disable overriding the global SNMP users.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global SNMPv3 users.</td></tr><tr><td><i>disable</i></td><td>Use the global SNMPv3 users.</td></tr></table>	Option	Description	<i>enable</i>	Override the global SNMPv3 users.	<i>disable</i>	Use the global SNMPv3 users.		
Option	Description								
<i>enable</i>	Override the global SNMPv3 users.								
<i>disable</i>	Use the global SNMPv3 users.								
owner-vdom	VDOM which owner of port belongs to.	string	Maximum length: 31						
poe-detection-type	PoE detection type for FortiSwitch. Read-only.	integer	Minimum value: 0 Maximum value: 255						
poe-lldp-detection	Enable/disable PoE LLDP detection.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable PoE LLDP detection.	
	<i>disable</i>	Disable PoE LLDP detection.	
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-
	Option	Description	
	<i>enable</i>	Enable PoE pre-standard detection.	
	<i>disable</i>	Disable PoE pre-standard detection.	
pre-provisioned	Pre-provisioned managed switch.	integer	Minimum value: 0 Maximum value: 255
staged-image-version	Staged image version for FortiSwitch.	string	Maximum length: 127
switch-device-tag	User definable label/tag.	string	Maximum length: 32
switch-id	Managed-switch id.	string	Maximum length: 16
switch-profile	FortiSwitch profile.	string	Maximum length: 35
type	Indication of switch type, physical or virtual.	option	-
	Option	Description	
	<i>virtual</i>	Switch is of type virtual.	
	<i>physical</i>	Switch is of type physical.	
version	FortiSwitch version.	integer	Minimum value: 0 Maximum value: 255

config 802-1X-settings

Parameter	Description	Type	Size
link-down-auth	Authentication state to set if a link is down.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.	
	<i>no-action</i>	Interface reauthentication is not needed.	
local-override	Enable to override global 802.1X settings on individual FortiSwitches.	option	-
	Option	Description	
	<i>enable</i>	Override global 802.1X settings.	
	<i>disable</i>	Use global 802.1X settings.	
max-reauth-attempt	Maximum number of authentication attempts (0 - 15, default = 3).	integer	Minimum value: 0 Maximum value: 15
reauth-period	Reauthentication time interval (1 - 1440 min, default = 60, 0 = disable).	integer	Minimum value: 0 Maximum value: 1440

config custom-command

Parameter	Description	Type	Size
command-entry	List of FortiSwitch commands.	string	Maximum length: 35
command-name	Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller custom-command.	string	Maximum length: 35

config igmp-snooping

Parameter	Description	Type	Size
aging-time	Maximum time to retain a multicast snooping entry for which no packets have been seen (15 - 3600 sec, default = 300).	integer	Minimum value: 15 Maximum value: 3600
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable unknown multicast flooding.	
	<i>disable</i>	Disable unknown multicast flooding.	
local-override	Enable/disable overriding the global IGMP snooping configuration.	option	-
	Option	Description	
	<i>enable</i>	Override the global IGMP snooping configuration.	
	<i>disable</i>	Use the global IGMP snooping configuration.	

config mirror

Parameter	Description	Type	Size
dst	Destination port.	string	Maximum length: 63
name	Mirror name.	string	Maximum length: 63
src-egress <name>	Source egress interfaces. Interface name.	string	Maximum length: 79
src-ingress <name>	Source ingress interfaces. Interface name.	string	Maximum length: 79
status	Active/inactive mirror configuration.	option	-
	Option	Description	
	<i>active</i>	Activate mirror configuration.	
	<i>inactive</i>	Deactivate mirror configuration.	
switching-packet	Enable/disable switching functionality when mirroring.	option	-
	Option	Description	
	<i>enable</i>	Enable switching functionality when mirroring.	
	<i>disable</i>	Disable switching functionality when mirroring.	

config ports

Parameter	Description	Type	Size						
allowed-vlans <vlan-name>	Configure switch port tagged vlans VLAN name.	string	Maximum length: 79						
allowed-vlans- all	Enable/disable all defined vlans on this port.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable all defined VLANs on this port.</td></tr><tr><td><i>disable</i></td><td>Disable all defined VLANs on this port.</td></tr></table>	Option	Description	<i>enable</i>	Enable all defined VLANs on this port.	<i>disable</i>	Disable all defined VLANs on this port.		
Option	Description								
<i>enable</i>	Enable all defined VLANs on this port.								
<i>disable</i>	Disable all defined VLANs on this port.								
arp-inspection- trust	Trusted or untrusted dynamic ARP inspection.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>untrusted</i></td><td>Untrusted dynamic ARP inspection.</td></tr><tr><td><i>trusted</i></td><td>Trusted dynamic ARP inspection.</td></tr></table>	Option	Description	<i>untrusted</i>	Untrusted dynamic ARP inspection.	<i>trusted</i>	Trusted dynamic ARP inspection.		
Option	Description								
<i>untrusted</i>	Untrusted dynamic ARP inspection.								
<i>trusted</i>	Trusted dynamic ARP inspection.								
bundle	Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable bundling.</td></tr><tr><td><i>disable</i></td><td>Disable bundling.</td></tr></table>	Option	Description	<i>enable</i>	Enable bundling.	<i>disable</i>	Disable bundling.		
Option	Description								
<i>enable</i>	Enable bundling.								
<i>disable</i>	Disable bundling.								
description	Description for port.	string	Maximum length: 63						
dhcp-snoop- option82-trust	Enable/disable allowance of DHCP with option-82 on untrusted interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowance of DHCP with option-82 on untrusted interface.</td></tr><tr><td><i>disable</i></td><td>Disable allowance of DHCP with option-82 on untrusted interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.	<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.		
Option	Description								
<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.								
<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.								
dhcp-snooping	Trusted or untrusted DHCP-snooping interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>untrusted</i></td><td>Untrusted DHCP snooping interface.</td></tr><tr><td><i>trusted</i></td><td>Trusted DHCP snooping interface.</td></tr></table>	Option	Description	<i>untrusted</i>	Untrusted DHCP snooping interface.	<i>trusted</i>	Trusted DHCP snooping interface.		
Option	Description								
<i>untrusted</i>	Untrusted DHCP snooping interface.								
<i>trusted</i>	Trusted DHCP snooping interface.								
discard-mode	Configure discard mode for port.	option	-						

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Discard disabled.</td></tr><tr><td><i>all-untagged</i></td><td>Discard all frames that are untagged.</td></tr><tr><td><i>all-tagged</i></td><td>Discard all frames that are tagged.</td></tr></table>	Option	Description	<i>none</i>	Discard disabled.	<i>all-untagged</i>	Discard all frames that are untagged.	<i>all-tagged</i>	Discard all frames that are tagged.		
	Option	Description									
	<i>none</i>	Discard disabled.									
	<i>all-untagged</i>	Discard all frames that are untagged.									
<i>all-tagged</i>	Discard all frames that are tagged.										
edge-port	Enable/disable this interface as an edge port, bridging connections between workstations and/or computers.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this interface as an edge port.</td></tr><tr><td><i>disable</i></td><td>Disable this interface as an edge port.</td></tr></table>	Option	Description	<i>enable</i>	Enable this interface as an edge port.	<i>disable</i>	Disable this interface as an edge port.				
	Option	Description									
	<i>enable</i>	Enable this interface as an edge port.									
<i>disable</i>	Disable this interface as an edge port.										
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								
export-to	Export managed-switch port to a tenant VDOM.	string	Maximum length: 31								
export-to-pool	Switch controller export port to pool-list.	string	Maximum length: 35								
fgt-peer-device-name	FGT peer device name. Read-only.	string	Maximum length: 16								
fgt-peer-port-name	FGT peer port name. Read-only.	string	Maximum length: 15								
fiber-port	Fiber-port. Read-only.	integer	Minimum value: 0 Maximum value: 1								
flags	Port properties flags. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
fortilink-port	FortiLink uplink port. Read-only.	integer	Minimum value: 0 Maximum value: 1								

Parameter	Description	Type	Size						
igmp-snooping	Set IGMP snooping mode for the physical port interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Interface takes part in IGMP snooping.</td></tr><tr><td><i>disable</i></td><td>Interface does not take part in IGMP snooping.</td></tr></table>	Option	Description	<i>enable</i>	Interface takes part in IGMP snooping.	<i>disable</i>	Interface does not take part in IGMP snooping.		
Option	Description								
<i>enable</i>	Interface takes part in IGMP snooping.								
<i>disable</i>	Interface does not take part in IGMP snooping.								
igmps-flood-reports	Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable flooding of IGMP snooping reports to this interface.</td></tr><tr><td><i>disable</i></td><td>Disable flooding of IGMP snooping reports to this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.	<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.		
Option	Description								
<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.								
<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.								
igmps-flood-traffic	Enable/disable flooding of IGMP snooping traffic to this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable flooding of IGMP snooping traffic to this interface.</td></tr><tr><td><i>disable</i></td><td>Disable flooding of IGMP snooping traffic to this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.	<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.		
Option	Description								
<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.								
<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.								
isl-local-trunk-name	ISL local trunk name. Read-only.	string	Maximum length: 15						
isl-peer-device-name	ISL peer device name. Read-only.	string	Maximum length: 16						
isl-peer-port-name	ISL peer port name. Read-only.	string	Maximum length: 15						
lacp-speed	end Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second (fast).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>slow</i></td><td>Send LACP message every 30 seconds.</td></tr><tr><td><i>fast</i></td><td>Send LACP message every second.</td></tr></table>	Option	Description	<i>slow</i>	Send LACP message every 30 seconds.	<i>fast</i>	Send LACP message every second.		
Option	Description								
<i>slow</i>	Send LACP message every 30 seconds.								
<i>fast</i>	Send LACP message every second.								
learning-limit	Limit the number of dynamic MAC addresses on this Port (1 - 128, 0 = no limit, default).	integer	Minimum value: 0 Maximum value: 128						
lldp-profile	LLDP port TLV profile.	string	Maximum length: 63						

Parameter	Description	Type	Size
lldp-status	LLDP transmit and receive status.	option	-

Option	Description
<i>disable</i>	Disable LLDP TX and RX.
<i>rx-only</i>	Enable LLDP as RX only.
<i>tx-only</i>	Enable LLDP as TX only.
<i>tx-rx</i>	Enable LLDP TX and RX.

loop-guard	Enable/disable loop-guard on this interface, an STP optimization used to prevent network loops.	option	-

Option	Description
<i>enabled</i>	Enable loop-guard on this interface.
<i>disabled</i>	Disable loop-guard on this interface.

loop-guard-timeout	Loop-guard timeout (0 - 120 min, default = 45).	integer	Minimum value: 0 Maximum value: 120

mac-addr	Port/Trunk MAC.	mac-address	Not Specified

max-bundle	Maximum size of LAG bundle (1 - 24, default = 24)	integer	Minimum value: 1 Maximum value: 24

mclag	Enable/disable multi-chassis link aggregation (MCLAG).	option	-

Option	Description
<i>enable</i>	Enable MCLAG.
<i>disable</i>	Disable MCLAG.

member-withdrawal-behavior	Port behavior after it withdraws because of loss of control packets.	option	-

Option	Description
<i>forward</i>	Forward traffic.
<i>block</i>	Block traffic.

Parameter	Description	Type	Size
members <member-name>	Aggregated LAG bundle interfaces. Interface name from available options.	string	Maximum length: 79
min-bundle	Minimum size of LAG bundle (1 - 24, default = 1)	integer	Minimum value: 1 Maximum value: 24
mode	LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.	option	-
	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.	
packet-sample-rate	Packet sampling rate (0 - 99999 p/sec).	integer	Minimum value: 0 Maximum value: 99999
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.	
poe-capable	PoE capable.	integer	Minimum value: 0 Maximum value: 1
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.	
poe-status	Enable/disable PoE status.	option	-

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PoE status.</td></tr><tr><td><i>disable</i></td><td>Disable PoE status.</td></tr></table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.										
	Option	Description															
	<i>enable</i>	Enable PoE status.															
<i>disable</i>	Disable PoE status.																
port-name	Switch port name.	string	Maximum length: 15														
port-number	Port number. Read-only.	integer	Minimum value: 1 Maximum value: 64														
port-owner	Switch port name.	string	Maximum length: 15														
port-prefix-type	Port prefix type. Read-only.	integer	Minimum value: 0 Maximum value: 1														
port-security-policy	Switch controller authentication policy to apply to this managed switch from available options.	string	Maximum length: 31														
port-selection-criteria	Algorithm for aggregate port selection.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>src-mac</i></td><td>Source MAC address.</td></tr><tr><td><i>dst-mac</i></td><td>Destination MAC address.</td></tr><tr><td><i>src-dst-mac</i></td><td>Source and destination MAC address.</td></tr><tr><td><i>src-ip</i></td><td>Source IP address.</td></tr><tr><td><i>dst-ip</i></td><td>Destination IP address.</td></tr><tr><td><i>src-dst-ip</i></td><td>Source and destination IP address.</td></tr></table>	Option	Description	<i>src-mac</i>	Source MAC address.	<i>dst-mac</i>	Destination MAC address.	<i>src-dst-mac</i>	Source and destination MAC address.	<i>src-ip</i>	Source IP address.	<i>dst-ip</i>	Destination IP address.	<i>src-dst-ip</i>	Source and destination IP address.		
	Option	Description															
	<i>src-mac</i>	Source MAC address.															
	<i>dst-mac</i>	Destination MAC address.															
	<i>src-dst-mac</i>	Source and destination MAC address.															
	<i>src-ip</i>	Source IP address.															
	<i>dst-ip</i>	Destination IP address.															
<i>src-dst-ip</i>	Source and destination IP address.																
qos-policy	Switch controller QoS policy from available options.	string	Maximum length: 63														
sample-direction	Packet sampling direction.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tx</i></td><td>Monitor transmitted traffic.</td></tr><tr><td><i>rx</i></td><td>Monitor received traffic.</td></tr><tr><td><i>both</i></td><td>Monitor transmitted and received traffic.</td></tr></table>	Option	Description	<i>tx</i>	Monitor transmitted traffic.	<i>rx</i>	Monitor received traffic.	<i>both</i>	Monitor transmitted and received traffic.								
	Option	Description															
	<i>tx</i>	Monitor transmitted traffic.															
	<i>rx</i>	Monitor received traffic.															
<i>both</i>	Monitor transmitted and received traffic.																

Parameter	Description	Type	Size
sflow-counter-interval	sFlow sampling counter polling interval (0 - 255 sec).	integer	Minimum value: 0 Maximum value: 255
speed	Switch port speed; default and available settings depend on hardware.	option	-

Option	Description
<i>10half</i>	10M half-duplex.
<i>10full</i>	10M full-duplex.
<i>100half</i>	100M half-duplex.
<i>100full</i>	100M full-duplex.
<i>1000auto</i>	Auto-negotiation (1G full-duplex only).
<i>1000fiber</i>	1G full-duplex (fiber SFPs only)
<i>1000full</i>	1G full-duplex
<i>10000</i>	10G full-duplex
<i>40000</i>	40G full-duplex
<i>auto</i>	Auto-negotiation.
<i>auto-module</i>	Auto Module.
<i>100FX-half</i>	100Mbps half-duplex. 100Base-FX.
<i>100FX-full</i>	100Mbps full-duplex. 100Base-FX.
<i>100000full</i>	100Gbps full-duplex.
<i>2500auto</i>	Auto-Negotiation (2.5Gbps Only).
<i>25000full</i>	25Gbps full-duplex.
<i>50000full</i>	50Gbps full-duplex.
<i>10000cr</i>	10Gbps copper interface.
<i>10000sr</i>	10Gbps SFI interface.
<i>100000sr4</i>	100Gbps SFI interface.
<i>100000cr4</i>	100Gbps copper interface.
<i>25000cr4</i>	25Gbps copper interface.
<i>25000sr4</i>	25Gbps SFI interface.
<i>5000full</i>	5Gbps full-duplex.

Parameter	Description	Type	Size						
stacking-port	Stacking port. Read-only.	integer	Minimum value: 0 Maximum value: 1						
status	Switch port admin status: up or down.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>up</td><td>Set admin status up.</td></tr><tr><td>down</td><td>Set admin status down.</td></tr></table>	Option	Description	up	Set admin status up.	down	Set admin status down.		
Option	Description								
up	Set admin status up.								
down	Set admin status down.								
sticky-mac	Enable or disable sticky-mac on the interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sticky mac on the interface.</td></tr><tr><td>disable</td><td>Disable sticky mac on the interface.</td></tr></table>	Option	Description	enable	Enable sticky mac on the interface.	disable	Disable sticky mac on the interface.		
Option	Description								
enable	Enable sticky mac on the interface.								
disable	Disable sticky mac on the interface.								
storm-control-policy	Switch controller storm control policy from available options.	string	Maximum length: 63						
stp-bpdu-guard	Enable/disable STP BPDU guard on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enabled</td><td>Enable STP BPDU guard on this interface.</td></tr><tr><td>disabled</td><td>Disable STP BPDU guard on this interface.</td></tr></table>	Option	Description	enabled	Enable STP BPDU guard on this interface.	disabled	Disable STP BPDU guard on this interface.		
Option	Description								
enabled	Enable STP BPDU guard on this interface.								
disabled	Disable STP BPDU guard on this interface.								
stp-bpdu-guard-timeout	BPDU Guard disabling protection (0 - 120 min).	integer	Minimum value: 0 Maximum value: 120						
stp-root-guard	Enable/disable STP root guard on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enabled</td><td>Enable STP root-guard on this interface.</td></tr><tr><td>disabled</td><td>Disable STP root-guard on this interface.</td></tr></table>	Option	Description	enabled	Enable STP root-guard on this interface.	disabled	Disable STP root-guard on this interface.		
Option	Description								
enabled	Enable STP root-guard on this interface.								
disabled	Disable STP root-guard on this interface.								
stp-state	Enable/disable Spanning Tree Protocol (STP) on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enabled</td><td>Enable STP on this interface.</td></tr><tr><td>disabled</td><td>Disable STP on this interface.</td></tr></table>	Option	Description	enabled	Enable STP on this interface.	disabled	Disable STP on this interface.		
Option	Description								
enabled	Enable STP on this interface.								
disabled	Disable STP on this interface.								

Parameter	Description	Type	Size
switch-id	Switch id. Read-only.	string	Maximum length: 16
type	Interface type: physical or trunk port.	option	-
	Option	Description	
	<i>physical</i>	Physical port.	
	<i>trunk</i>	Trunk port.	
untagged-vlans <vlan-name>	Configure switch port untagged vlans VLAN name.	string	Maximum length: 79
vlan	Assign switch ports to a VLAN.	string	Maximum length: 15

config remote-log

Parameter	Description	Type	Size																						
csv	Enable/disable comma-separated value (CSV) strings.	option	-																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable comma-separated value (CSV) strings.</td></tr><tr><td><i>disable</i></td><td>Disable comma-separated value (CSV) strings.</td></tr></table>	Option	Description	<i>enable</i>	Enable comma-separated value (CSV) strings.	<i>disable</i>	Disable comma-separated value (CSV) strings.																		
Option	Description																								
<i>enable</i>	Enable comma-separated value (CSV) strings.																								
<i>disable</i>	Disable comma-separated value (CSV) strings.																								
facility	Facility to log to remote syslog server.	option	-																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslogd.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>UUCP server messages.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr></table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslogd.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	UUCP server messages.	<i>cron</i>	Clock daemon.		
Option	Description																								
<i>kernel</i>	Kernel messages.																								
<i>user</i>	Random user-level messages.																								
<i>mail</i>	Mail system.																								
<i>daemon</i>	System daemons.																								
<i>auth</i>	Security/authorization messages.																								
<i>syslog</i>	Messages generated internally by syslogd.																								
<i>lpr</i>	Line printer subsystem.																								
<i>news</i>	Network news subsystem.																								
<i>uucp</i>	UUCP server messages.																								
<i>cron</i>	Clock daemon.																								

Parameter	Description	Type	Size

Option	Description
<i>authpriv</i>	Security/authorization messages (private).
<i>ftp</i>	FTP daemon.
<i>ntp</i>	NTP daemon.
<i>audit</i>	Log audit.
<i>alert</i>	Log alert.
<i>clock</i>	Clock daemon.
<i>local0</i>	Reserved for local use.
<i>local1</i>	Reserved for local use.
<i>local2</i>	Reserved for local use.
<i>local3</i>	Reserved for local use.
<i>local4</i>	Reserved for local use.
<i>local5</i>	Reserved for local use.
<i>local6</i>	Reserved for local use.
<i>local7</i>	Reserved for local use.

name	Remote log name.	string	Maximum length: 35
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535
server	IPv4 address of the remote syslog server.	string	Maximum length: 63
severity	Severity of logs to be transferred to remote log server.	option	-

Option	Description
<i>emergency</i>	Emergency level.
<i>alert</i>	Alert level.
<i>critical</i>	Critical level.
<i>error</i>	Error level.
<i>warning</i>	Warning level.

Parameter	Description	Type	Size
	Option	Description	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-
	Option	Description	
	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.	
	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.	

config snmp-community

Parameter	Description	Type	Size
events	SNMP notifications (traps) to send.	option	-
	Option	Description	
	<i>cpu-high</i>	Send a trap when CPU usage too high.	
	<i>mem-low</i>	Send a trap when available memory is low.	
	<i>log-full</i>	Send a trap when log disk space becomes low.	
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.	
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).	
id	SNMP community ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	SNMP community name.	string	Maximum length: 35
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535
query-v1-status	Enable/disable SNMP v1 queries.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP v1 queries.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP v1 queries.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP v1 queries.	<i>enable</i>	Enable SNMP v1 queries.		
	Option	Description							
	<i>disable</i>	Disable SNMP v1 queries.							
<i>enable</i>	Enable SNMP v1 queries.								
query-v2c-port	SNMP v2c query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP v2c queries.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP v2c queries.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP v2c queries.	<i>enable</i>	Enable SNMP v2c queries.		
	Option	Description							
	<i>disable</i>	Disable SNMP v2c queries.							
<i>enable</i>	Enable SNMP v2c queries.								
status	Enable/disable this SNMP community.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP community.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP community.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP community.	<i>enable</i>	Enable SNMP community.		
	Option	Description							
	<i>disable</i>	Disable SNMP community.							
<i>enable</i>	Enable SNMP community.								
trap-v1-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535						
trap-v1-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP v1 traps.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP v1 traps.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP v1 traps.	<i>enable</i>	Enable SNMP v1 traps.		
	Option	Description							
	<i>disable</i>	Disable SNMP v1 traps.							
<i>enable</i>	Enable SNMP v1 traps.								
trap-v2c-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535						

Parameter	Description	Type	Size
trap-v2c-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-

Option	Description
<i>disable</i>	Disable SNMP v2c traps.
<i>enable</i>	Enable SNMP v2c traps.

config hosts

Parameter	Description	Type	Size
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IPv4 address of the SNMP manager (host).	user	Not Specified

config snmp-sysinfo

Parameter	Description	Type	Size
contact-info	Contact information.	string	Maximum length: 35
description	System description.	string	Maximum length: 35
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24
location	System location.	string	Maximum length: 35
status	Enable/disable SNMP.	option	-

Option	Description
<i>disable</i>	Disable SNMP.
<i>enable</i>	Enable SNMP.

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-log-full-threshold	Log disk 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

config snmp-user

Parameter	Description	Type	Size
auth-proto	Authentication protocol.	option	-
	Option	Description	
	<i>md5</i>	HMAC-MD5-96 authentication protocol.	
	<i>sha</i>	HMAC-SHA-96 authentication protocol.	
auth-pwd	Password for authentication protocol.	password	Not Specified
name	SNMP user name.	string	Maximum length: 32
priv-proto	Privacy (encryption) protocol.	option	-
	Option	Description	
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	
	<i>des</i>	CBC-DES symmetric encryption protocol.	
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified
queries	Enable/disable SNMP queries for this user.	option	-
	Option	Description	
	<i>disable</i>	Disable SNMP queries for this user.	

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SNMP queries for this user.</td></tr></table>			Option	Description	<i>enable</i>	Enable SNMP queries for this user.				
Option	Description										
<i>enable</i>	Enable SNMP queries for this user.										
query-port	SNMPv3 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535								
security-level	Security level for message authentication and encryption.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-auth-no-priv</i></td><td>Message with no authentication and no privacy (encryption).</td></tr><tr><td><i>auth-no-priv</i></td><td>Message with authentication but no privacy (encryption).</td></tr><tr><td><i>auth-priv</i></td><td>Message with authentication and privacy (encryption).</td></tr></table>			Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).
Option	Description										
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).										
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).										
<i>auth-priv</i>	Message with authentication and privacy (encryption).										

config static-mac

Parameter	Description	Type	Size						
description	Description.	string	Maximum length: 63						
id	Id	integer	Minimum value: 0 Maximum value: 4294967295						
interface	Interface name.	string	Maximum length: 35						
mac	MAC address.	mac-address	Not Specified						
type	Type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Static MAC.</td></tr><tr><td>sticky</td><td>Sticky MAC.</td></tr></table>			Option	Description	static	Static MAC.	sticky	Sticky MAC.
Option	Description								
static	Static MAC.								
sticky	Sticky MAC.								
vlan	Vlan.	string	Maximum length: 15						

config storm-control

Parameter	Description	Type	Size						
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Drop broadcast traffic.</td></tr><tr><td><i>disable</i></td><td>Allow broadcast traffic.</td></tr></table>	Option	Description	<i>enable</i>	Drop broadcast traffic.	<i>disable</i>	Allow broadcast traffic.		
Option	Description								
<i>enable</i>	Drop broadcast traffic.								
<i>disable</i>	Allow broadcast traffic.								
local-override	Enable to override global FortiSwitch storm control settings for this FortiSwitch.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override global storm control settings.</td></tr><tr><td><i>disable</i></td><td>Use global storm control settings.</td></tr></table>	Option	Description	<i>enable</i>	Override global storm control settings.	<i>disable</i>	Use global storm control settings.		
Option	Description								
<i>enable</i>	Override global storm control settings.								
<i>disable</i>	Use global storm control settings.								
rate	Rate in packets per second at which storm traffic is controlled (1 - 10000000, default = 500). Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000						
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Drop unknown multicast traffic.</td></tr><tr><td><i>disable</i></td><td>Allow unknown multicast traffic.</td></tr></table>	Option	Description	<i>enable</i>	Drop unknown multicast traffic.	<i>disable</i>	Allow unknown multicast traffic.		
Option	Description								
<i>enable</i>	Drop unknown multicast traffic.								
<i>disable</i>	Allow unknown multicast traffic.								
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Drop unknown unicast traffic.</td></tr><tr><td><i>disable</i></td><td>Allow unknown unicast traffic.</td></tr></table>	Option	Description	<i>enable</i>	Drop unknown unicast traffic.	<i>disable</i>	Allow unknown unicast traffic.		
Option	Description								
<i>enable</i>	Drop unknown unicast traffic.								
<i>disable</i>	Allow unknown unicast traffic.								

config stp-instance

Parameter	Description	Type	Size
id	Instance ID.	string	Maximum length: 2
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 stp-settings

Parameter	Description	Type	Size

forward-time	Period of time a port is in listening and learning state (4 - 30 sec, default = 15).	integer	Minimum value: 4 Maximum value: 30
hello-time	Period of time between successive STP frame Bridge Protocol Data Units (BPDUs) sent on a port (1 - 10 sec, default = 2).	integer	Minimum value: 1 Maximum value: 10
local-override	Enable to configure local STP settings that override global STP settings.	option	-

Option	Description
<i>enable</i>	Override global STP settings.
<i>disable</i>	Use global STP settings.

Parameter	Description	Type	Size
max-age	Maximum time before a bridge port saves its configuration BPDU information (6 - 40 sec, default = 20).	integer	Minimum value: 6 Maximum value: 40
max-hops	Maximum number of hops between the root bridge and the furthest bridge (1- 40, default = 20).	integer	Minimum value: 1 Maximum value: 40
name	Name of local STP settings configuration.	string	Maximum length: 31
pending-timer	Pending time (1 - 15 sec, default = 4).	integer	Minimum value: 1 Maximum value: 15
revision	STP revision number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535

config switch-log

Parameter	Description	Type	Size
local-override	Enable to configure local logging settings that override global logging settings.	option	-
	Option	Description	
	<i>enable</i>	Override global logging settings.	
	<i>disable</i>	Use global logging settings.	
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	

Parameter	Description	Type	Size
	Option	Description	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
status	Enable/disable adding FortiSwitch logs to the FortiGate event log.	option	-
	Option	Description	
	<i>enable</i>	Add FortiSwitch logs to the FortiGate event log.	
	<i>disable</i>	Do not add FortiSwitch logs to the FortiGate event log.	

config switch-controller network-monitor-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure network monitor settings.

```
config switch-controller network-monitor-settings
    Description: Configure network monitor settings.
    set network-monitoring [enable|disable]
end
```

config switch-controller network-monitor-settings

Parameter	Description	Type	Size						
network-monitoring	Enable/disable passive gathering of information by FortiSwitch units concerning other network devices.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable network monitoring on FortiSwitch.</td></tr><tr><td><i>disable</i></td><td>Disable network monitoring on FortiSwitch.</td></tr></table>	Option	Description	<i>enable</i>	Enable network monitoring on FortiSwitch.	<i>disable</i>	Disable network monitoring on FortiSwitch.		
Option	Description								
<i>enable</i>	Enable network monitoring on FortiSwitch.								
<i>disable</i>	Disable network monitoring on FortiSwitch.								

config switch-controller qos dot1p-map



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS 802.1p.

```
config switch-controller qos dot1p-map
  Description: Configure FortiSwitch QoS 802.1p.
  edit <name>
    set description {string}
    set egress-pri-tagging [disable|enable]
    set priority-0 [queue-0|queue-1|...]
    set priority-1 [queue-0|queue-1|...]
    set priority-2 [queue-0|queue-1|...]
```

```

set priority-3 [queue-0|queue-1|...]
set priority-4 [queue-0|queue-1|...]
set priority-5 [queue-0|queue-1|...]
set priority-6 [queue-0|queue-1|...]
set priority-7 [queue-0|queue-1|...]
next
end

```

config switch-controller qos dot1p-map

Parameter	Description	Type	Size
description	Description of the 802.1p name.	string	Maximum length: 63
egress-pri-tagging	Enable/disable egress priority-tag frame.	option	-
	Option	Description	
	<i>disable</i>	Disable egress priority tagging.	
	<i>enable</i>	Enable egress priority tagging.	
name	Dot1p map name.	string	Maximum length: 63
priority-0	COS queue mapped to dot1p priority number.	option	-
	Option	Description	
	<i>queue-0</i>	COS queue 0 (lowest priority).	
	<i>queue-1</i>	COS queue 1.	
	<i>queue-2</i>	COS queue 2.	
	<i>queue-3</i>	COS queue 3.	
	<i>queue-4</i>	COS queue 4.	
	<i>queue-5</i>	COS queue 5.	
	<i>queue-6</i>	COS queue 6.	
	<i>queue-7</i>	COS queue 7 (highest priority).	
priority-1	COS queue mapped to dot1p priority number.	option	-
	Option	Description	
	<i>queue-0</i>	COS queue 0 (lowest priority).	
	<i>queue-1</i>	COS queue 1.	
	<i>queue-2</i>	COS queue 2.	

Parameter	Description	Type	Size

Option	Description
<i>queue-3</i>	COS queue 3.
<i>queue-4</i>	COS queue 4.
<i>queue-5</i>	COS queue 5.
<i>queue-6</i>	COS queue 6.
<i>queue-7</i>	COS queue 7 (highest priority).

priority-2	COS queue mapped to dot1p priority number.	option	-

Option	Description
<i>queue-0</i>	COS queue 0 (lowest priority).
<i>queue-1</i>	COS queue 1.
<i>queue-2</i>	COS queue 2.
<i>queue-3</i>	COS queue 3.
<i>queue-4</i>	COS queue 4.
<i>queue-5</i>	COS queue 5.
<i>queue-6</i>	COS queue 6.
<i>queue-7</i>	COS queue 7 (highest priority).

priority-3	COS queue mapped to dot1p priority number.	option	-

Option	Description
<i>queue-0</i>	COS queue 0 (lowest priority).
<i>queue-1</i>	COS queue 1.
<i>queue-2</i>	COS queue 2.
<i>queue-3</i>	COS queue 3.
<i>queue-4</i>	COS queue 4.
<i>queue-5</i>	COS queue 5.
<i>queue-6</i>	COS queue 6.
<i>queue-7</i>	COS queue 7 (highest priority).

priority-4	COS queue mapped to dot1p priority number.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>queue-0</i>	COS queue 0 (lowest priority).	
	<i>queue-1</i>	COS queue 1.	
	<i>queue-2</i>	COS queue 2.	
	<i>queue-3</i>	COS queue 3.	
	<i>queue-4</i>	COS queue 4.	
	<i>queue-5</i>	COS queue 5.	
	<i>queue-6</i>	COS queue 6.	
	<i>queue-7</i>	COS queue 7 (highest priority).	
priority-5	COS queue mapped to dot1p priority number.	option	-
	Option	Description	
	<i>queue-0</i>	COS queue 0 (lowest priority).	
	<i>queue-1</i>	COS queue 1.	
	<i>queue-2</i>	COS queue 2.	
	<i>queue-3</i>	COS queue 3.	
	<i>queue-4</i>	COS queue 4.	
	<i>queue-5</i>	COS queue 5.	
	<i>queue-6</i>	COS queue 6.	
	<i>queue-7</i>	COS queue 7 (highest priority).	
priority-6	COS queue mapped to dot1p priority number.	option	-
	Option	Description	
	<i>queue-0</i>	COS queue 0 (lowest priority).	
	<i>queue-1</i>	COS queue 1.	
	<i>queue-2</i>	COS queue 2.	
	<i>queue-3</i>	COS queue 3.	
	<i>queue-4</i>	COS queue 4.	
	<i>queue-5</i>	COS queue 5.	
	<i>queue-6</i>	COS queue 6.	
	<i>queue-7</i>	COS queue 7 (highest priority).	

Parameter	Description	Type	Size
priority-7	COS queue mapped to dot1p priority number.	option	-

Option	Description
<i>queue-0</i>	COS queue 0 (lowest priority).
<i>queue-1</i>	COS queue 1.
<i>queue-2</i>	COS queue 2.
<i>queue-3</i>	COS queue 3.
<i>queue-4</i>	COS queue 4.
<i>queue-5</i>	COS queue 5.
<i>queue-6</i>	COS queue 6.
<i>queue-7</i>	COS queue 7 (highest priority).

config switch-controller qos ip-dscp-map



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS IP precedence/DSCP.

```

config switch-controller qos ip-dscp-map
  Description: Configure FortiSwitch QoS IP precedence/DSCP.
  edit <name>
    set description {string}
    config map
      Description: Maps between IP-DSCP value to COS queue.
      edit <name>
        set cos-queue {integer}
        set diffserv {option1}, {option2}, ...
        set ip-precedence {option1}, {option2}, ...
        set value {user}
      next
    end
  next
end

```

config switch-controller qos ip-dscp-map

Parameter	Description	Type	Size
description	Description of the ip-dscp map name.	string	Maximum length: 63
name	Dscp map name.	string	Maximum length: 63

config map

Parameter	Description	Type	Size
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																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>AF22</td><td>DSCP AF22.</td></tr><tr><td>AF23</td><td>DSCP AF23.</td></tr><tr><td>CS3</td><td>DSCP CS3.</td></tr><tr><td>AF31</td><td>DSCP AF31.</td></tr><tr><td>AF32</td><td>DSCP AF32.</td></tr><tr><td>AF33</td><td>DSCP AF33.</td></tr><tr><td>CS4</td><td>DSCP CS4.</td></tr><tr><td>AF41</td><td>DSCP AF41.</td></tr><tr><td>AF42</td><td>DSCP AF42.</td></tr><tr><td>AF43</td><td>DSCP AF43.</td></tr><tr><td>CS5</td><td>DSCP CS5.</td></tr><tr><td>EF</td><td>DSCP EF.</td></tr><tr><td>CS6</td><td>DSCP CS6.</td></tr><tr><td>CS7</td><td>DSCP CS7.</td></tr></table>	Option	Description	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.		
	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	-																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>network-control</td><td>Network control.</td></tr><tr><td>internetwork-control</td><td>Internetwork control.</td></tr><tr><td>critic-ecp</td><td>Critic ECP.</td></tr><tr><td>flashoverride</td><td>Flash override.</td></tr><tr><td>flash</td><td>Flash.</td></tr><tr><td>immediate</td><td>Immediate.</td></tr><tr><td>priority</td><td>Priority.</td></tr><tr><td>routine</td><td>Routine.</td></tr></table>	Option	Description	network-control	Network control.	internetwork-control	Internetwork control.	critic-ecp	Critic ECP.	flashoverride	Flash override.	flash	Flash.	immediate	Immediate.	priority	Priority.	routine	Routine.														
	Option	Description																															
	network-control	Network control.																															
	internetwork-control	Internetwork control.																															
	critic-ecp	Critic ECP.																															
	flashoverride	Flash override.																															
	flash	Flash.																															
	immediate	Immediate.																															
	priority	Priority.																															
routine	Routine.																																
name	Dscp mapping entry name.	string	Maximum length: 63																														
value	Raw values of DSCP (0 - 63).	user	Not Specified																														

config switch-controller qos qos-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS policy.

```
config switch-controller qos qos-policy
    Description: Configure FortiSwitch QoS policy.
    edit <name>
        set default-cos {integer}
        set queue-policy {string}
        set trust-dot1p-map {string}
        set trust-ip-dscp-map {string}
    next
end
```

config switch-controller qos qos-policy

Parameter	Description	Type	Size
default-cos	Default cos queue for untagged packets.	integer	Minimum value: 0 Maximum value: 7

Parameter	Description	Type	Size
name	QoS policy name.	string	Maximum length: 63
queue-policy	QoS egress queue policy.	string	Maximum length: 63
trust-dot1p-map	QoS trust 802.1p map.	string	Maximum length: 63
trust-ip-dscp-map	QoS trust ip dscp map.	string	Maximum length: 63

config switch-controller qos queue-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS egress queue policy.

```
config switch-controller qos queue-policy
    Description: Configure FortiSwitch QoS egress queue policy.
    edit <name>
        config cos-queue
            Description: COS queue configuration.
            edit <name>
                set description {string}
                set drop-policy [taildrop|weighted-random-early-detection]
```

```

        set max-rate {integer}
        set max-rate-percent {integer}
        set min-rate {integer}
        set min-rate-percent {integer}
        set weight {integer}
    next
end
set rate-by [kbps|percent]
set schedule [strict|round-robin|...]
next
end

```

config switch-controller qos queue-policy

Parameter	Description	Type	Size
name	QoS policy name	string	Maximum length: 63
rate-by	COS queue rate by kbps or percent.	option	-
	Option	Description	
	<i>kbps</i>	Rate by kbps.	
	<i>percent</i>	Rate by percent.	
schedule	COS queue scheduling.	option	-
	Option	Description	
	<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).	
	<i>round-robin</i>	Round robin scheduling.	
	<i>weighted</i>	Weighted round robin scheduling.	

config cos-queue

Parameter	Description	Type	Size
description	Description of the COS queue.	string	Maximum length: 63
drop-policy	COS queue drop policy.	option	-
	Option	Description	
	<i>taildrop</i>	Taildrop policy.	
	<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.	

Parameter	Description	Type	Size
max-rate	Maximum rate (0 - 4294967295 kbps, 0 to disable).	integer	Minimum value: 0 Maximum value: 4294967295
max-rate-percent	Maximum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295
min-rate	Minimum rate (0 - 4294967295 kbps, 0 to disable).	integer	Minimum value: 0 Maximum value: 4294967295
min-rate-percent	Minimum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295
name	Cos queue ID.	string	Maximum length: 63
weight	Weight of weighted round robin scheduling.	integer	Minimum value: 0 Maximum value: 4294967295

config switch-controller quarantine



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch quarantine support.

```
config switch-controller quarantine
  Description: Configure FortiSwitch quarantine support.
  set quarantine [enable|disable]
  config targets
    Description: Quarantine MACs.
    edit <mac>
      set description {string}
      set tag <tags1>, <tags2>, ...
    next
  end
end
```

config switch-controller quarantine

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

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable quarantine.	
	<i>disable</i>	Disable quarantine.	

config targets

Parameter	Description	Type	Size
description	Description for the quarantine MAC.	string	Maximum length: 63
mac	Quarantine MAC.	mac-address	Not Specified
tag <tags>	Tags for the quarantine MAC. Tag string(eg. string1 string2 string3).	string	Maximum length: 63

config switch-controller remote-log



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure logging by FortiSwitch device to a remote syslog server.

```

config switch-controller remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
    edit <name>
        set csv [enable|disable]
        set facility [kernel|user|...]
        set port {integer}
        set server {string}
        set severity [emergency|alert|...]
        set status [enable|disable]
    next
end

```

config switch-controller remote-log

Parameter	Description	Type	Size																														
csv	Enable/disable comma-separated value (CSV) strings.	option	-																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable comma-separated value (CSV) strings.</td></tr><tr><td><i>disable</i></td><td>Disable comma-separated value (CSV) strings.</td></tr></table>	Option	Description	<i>enable</i>	Enable comma-separated value (CSV) strings.	<i>disable</i>	Disable comma-separated value (CSV) strings.																										
Option	Description																																
<i>enable</i>	Enable comma-separated value (CSV) strings.																																
<i>disable</i>	Disable comma-separated value (CSV) strings.																																
facility	Facility to log to remote syslog server.	option	-																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslogd.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>UUCP server messages.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr></table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslogd.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	UUCP server messages.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.		
Option	Description																																
<i>kernel</i>	Kernel messages.																																
<i>user</i>	Random user-level messages.																																
<i>mail</i>	Mail system.																																
<i>daemon</i>	System daemons.																																
<i>auth</i>	Security/authorization messages.																																
<i>syslog</i>	Messages generated internally by syslogd.																																
<i>lpr</i>	Line printer subsystem.																																
<i>news</i>	Network news subsystem.																																
<i>uucp</i>	UUCP server messages.																																
<i>cron</i>	Clock daemon.																																
<i>authpriv</i>	Security/authorization messages (private).																																
<i>ftp</i>	FTP daemon.																																
<i>ntp</i>	NTP daemon.																																
<i>audit</i>	Log audit.																																

Parameter	Description	Type	Size

	Option	Description	
	<i>alert</i>	Log alert.	
	<i>clock</i>	Clock daemon.	
	<i>local0</i>	Reserved for local use.	
	<i>local1</i>	Reserved for local use.	
	<i>local2</i>	Reserved for local use.	
	<i>local3</i>	Reserved for local use.	
	<i>local4</i>	Reserved for local use.	
	<i>local5</i>	Reserved for local use.	
	<i>local6</i>	Reserved for local use.	
	<i>local7</i>	Reserved for local use.	

name	Remote log name.	string	Maximum length: 35
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535
server	IPv4 address of the remote syslog server.	string	Maximum length: 63
severity	Severity of logs to be transferred to remote log server.	option	-

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

status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.	
	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.	

config switch-controller security-policy 802-1X



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure 802.1x MAC Authentication Bypass (MAB) policies.

```
config switch-controller security-policy 802-1X
  Description: Configure 802.1x MAC Authentication Bypass (MAB) policies.
  edit <name>
    set auth-fail-vlan [disable|enable]
    set auth-fail-vlan-id {string}
    set eap-passthru [disable|enable]
    set framevid-apply [disable|enable]
    set guest-auth-delay {integer}
    set guest-vlan [disable|enable]
    set guest-vlan-id {string}
    set mac-auth-bypass [disable|enable]
    set open-auth [disable|enable]
    set policy-type {option}
```

```

set radius-timeout-overwrite [disable|enable]
set security-mode [802.1X|802.1X-mac-based]
set user-group <name1>, <name2>, ...
next
end

```

config switch-controller security-policy 802-1X

Parameter	Description	Type	Size						
auth-fail-vlan	Enable to allow limited access to clients that cannot authenticate.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication fail VLAN on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable authentication fail VLAN on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication fail VLAN on this interface.	<i>enable</i>	Enable authentication fail VLAN on this interface.		
Option	Description								
<i>disable</i>	Disable authentication fail VLAN on this interface.								
<i>enable</i>	Enable authentication fail VLAN on this interface.								
auth-fail-vlan-id	VLAN ID on which authentication failed.	string	Maximum length: 15						
eap-passthru	Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for more flexible authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable EAP pass-through mode on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable EAP pass-through mode on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable EAP pass-through mode on this interface.	<i>enable</i>	Enable EAP pass-through mode on this interface.		
Option	Description								
<i>disable</i>	Disable EAP pass-through mode on this interface.								
<i>enable</i>	Enable EAP pass-through mode on this interface.								
framevid-apply	Enable/disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.</td></tr><tr><td><i>enable</i></td><td>Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.</td></tr></table>	Option	Description	<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
Option	Description								
<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.								
<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.								
guest-auth-delay	Guest authentication delay (1 - 900 sec, default = 30).	integer	Minimum value: 1 Maximum value: 900						
guest-vlan	Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable guest VLAN on this interface.	
	<i>enable</i>	Enable guest VLAN on this interface.	
guest-vlan-id	Guest VLAN name.	string	Maximum length: 15
mac-auth-bypass	Enable/disable MAB for this policy.	option	-
	Option	Description	
	<i>disable</i>	Disable MAB.	
	<i>enable</i>	Enable MAB.	
name	Policy name.	string	Maximum length: 31
open-auth	Enable/disable open authentication for this policy.	option	-
	Option	Description	
	<i>disable</i>	Disable open authentication.	
	<i>enable</i>	Enable open authentication.	
policy-type	Policy type.	option	-
	Option	Description	
	<i>802.1X</i>	802.1X security policy.	
radius-timeout-overwrite	Enable to override the global RADIUS session timeout.	option	-
	Option	Description	
	<i>disable</i>	Override the global RADIUS session timeout.	
	<i>enable</i>	Use the global RADIUS session timeout.	
security-mode	Port or MAC based 802.1X security mode.	option	-
	Option	Description	
	<i>802.1X</i>	802.1X port based authentication.	
	<i>802.1X-mac-based</i>	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

config switch-controller security-policy local-access



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

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 internal-allowaccess {option1}, {option2}, ...
        set mgmt-allowaccess {option1}, {option2}, ...
    next
end
```

config switch-controller security-policy local-access

Parameter	Description	Type	Size																
internal-allowaccess	Allowed access on the switch internal interface.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>radius-acct</td><td>RADIUS accounting access.</td></tr></table>	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.		
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.																		
mgmt-allowaccess	Allowed access on the switch management interface.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>radius-acct</td><td>RADIUS accounting access.</td></tr></table>	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.		
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.																		
name	Policy name.	string	Maximum length: 31																

config switch-controller sflow



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch sFlow.

```
config switch-controller sflow
    Description: Configure FortiSwitch sFlow.
    set collector-ip {ipv4-address}
    set collector-port {integer}
end
```

config switch-controller sflow

Parameter	Description	Type	Size
collector-ip	Collector IP.	ipv4-address	Not Specified
collector-port	SFlow collector port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535

config switch-controller snmp-community



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP v1/v2c communities globally.

```
config switch-controller snmp-community
  Description: Configure FortiSwitch SNMP v1/v2c communities globally.
  edit <id>
    set events {option1}, {option2}, ...
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ip {user}
      next
    end
    set name {string}
    set query-v1-port {integer}
    set query-v1-status [disable|enable]
    set query-v2c-port {integer}
    set query-v2c-status [disable|enable]
    set status [disable|enable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v1-status [disable|enable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set trap-v2c-status [disable|enable]
```

next
end

config switch-controller snmp-community

Parameter	Description	Type	Size												
events	SNMP notifications (traps) to send.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cpu-high</i></td><td>Send a trap when CPU usage too high.</td></tr><tr><td><i>mem-low</i></td><td>Send a trap when available memory is low.</td></tr><tr><td><i>log-full</i></td><td>Send a trap when log disk space becomes low.</td></tr><tr><td><i>intf-ip</i></td><td>Send a trap when an interface IP address is changed.</td></tr><tr><td><i>ent-conf-change</i></td><td>Send a trap when an entity MIB change occurs (RFC4133).</td></tr></table>	Option	Description	<i>cpu-high</i>	Send a trap when CPU usage too high.	<i>mem-low</i>	Send a trap when available memory is low.	<i>log-full</i>	Send a trap when log disk space becomes low.	<i>intf-ip</i>	Send a trap when an interface IP address is changed.	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	Option	Description													
	<i>cpu-high</i>	Send a trap when CPU usage too high.													
	<i>mem-low</i>	Send a trap when available memory is low.													
	<i>log-full</i>	Send a trap when log disk space becomes low.													
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.													
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).														
id	SNMP community ID.	integer	Minimum value: 0 Maximum value: 4294967295												
name	SNMP community name.	string	Maximum length: 35												
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535												
query-v1-status	Enable/disable SNMP v1 queries.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP v1 queries.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP v1 queries.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP v1 queries.	<i>enable</i>	Enable SNMP v1 queries.								
	Option	Description													
	<i>disable</i>	Disable SNMP v1 queries.													
<i>enable</i>	Enable SNMP v1 queries.														
query-v2c-port	SNMP v2c query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535												
query-v2c-status	Enable/disable SNMP v2c queries.	option	-												

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable SNMP v2c queries.	
	<i>enable</i>	Enable SNMP v2c queries.	
status	Enable/disable this SNMP community.	option	-
	Option	Description	
	<i>disable</i>	Disable SNMP community.	
	<i>enable</i>	Enable SNMP community.	
trap-v1-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535
trap-v1-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535
trap-v1-status	Enable/disable SNMP v1 traps.	option	-
	Option	Description	
	<i>disable</i>	Disable SNMP v1 traps.	
	<i>enable</i>	Enable SNMP v1 traps.	
trap-v2c-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-
	Option	Description	
	<i>disable</i>	Disable SNMP v2c traps.	
	<i>enable</i>	Enable SNMP v2c traps.	

config hosts

Parameter	Description	Type	Size
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IPv4 address of the SNMP manager (host).	user	Not Specified

config switch-controller snmp-sysinfo



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP system information globally.

```
config switch-controller snmp-sysinfo
    Description: Configure FortiSwitch SNMP system information globally.
    set contact-info {string}
    set description {string}
    set engine-id {string}
    set location {string}
    set status [disable|enable]
end
```

config switch-controller snmp-sysinfo

Parameter	Description	Type	Size
contact-info	Contact information.	string	Maximum length: 35
description	System description.	string	Maximum length: 35
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24
location	System location.	string	Maximum length: 35
status	Enable/disable SNMP.	option	-

Option	Description
<i>disable</i>	Disable SNMP.
<i>enable</i>	Enable SNMP.

config switch-controller snmp-trap-threshold



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP trap threshold values globally.

```
config switch-controller snmp-trap-threshold
  Description: Configure FortiSwitch SNMP trap threshold values globally.
  set trap-high-cpu-threshold {integer}
  set trap-log-full-threshold {integer}
  set trap-low-memory-threshold {integer}
end
```

config switch-controller snmp-trap-threshold

Parameter	Description	Type	Size
trap-high-cpu-threshold	CPU 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
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295

config switch-controller snmp-user



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP v3 users globally.

```
config switch-controller snmp-user
  Description: Configure FortiSwitch SNMP v3 users globally.
  edit <name>
    set auth-proto [md5|sha]
    set auth-pwd {password}
    set priv-proto [aes|des]
    set priv-pwd {password}
    set queries [disable|enable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
  next
end
```

config switch-controller snmp-user

Parameter	Description	Type	Size
auth-proto	Authentication protocol.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>md5</i>	HMAC-MD5-96 authentication protocol.	
	<i>sha</i>	HMAC-SHA-96 authentication protocol.	
auth-pwd	Password for authentication protocol.	password	Not Specified
name	SNMP user name.	string	Maximum length: 32
priv-proto	Privacy (encryption) protocol.	option	-
	Option	Description	
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	
	<i>des</i>	CBC-DES symmetric encryption protocol.	
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified
queries	Enable/disable SNMP queries for this user.	option	-
	Option	Description	
	<i>disable</i>	Disable SNMP queries for this user.	
	<i>enable</i>	Enable SNMP queries for this user.	
query-port	SNMPv3 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535
security-level	Security level for message authentication and encryption.	option	-
	Option	Description	
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	
	<i>auth-priv</i>	Message with authentication and privacy (encryption).	

config switch-controller storm-control



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch storm control.

```
config switch-controller storm-control
    Description: Configure FortiSwitch storm control.
    set broadcast [enable|disable]
    set rate {integer}
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
end
```

config switch-controller storm-control

Parameter	Description	Type	Size
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-
	Option	Description	
	<i>enable</i>	Enable broadcast storm control.	
	<i>disable</i>	Disable broadcast storm control.	

Parameter	Description	Type	Size
rate	Rate in packets per second at which storm traffic is controlled (1 - 10000000, default = 500). Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-

Option	Description
<i>enable</i>	Enable unknown multicast storm control.
<i>disable</i>	Disable unknown multicast storm control.

unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-

Option	Description
<i>enable</i>	Enable unknown unicast storm control.
<i>disable</i>	Disable unknown unicast storm control.

config switch-controller storm-control-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch storm control policy to be applied on managed-switch ports.

```
config switch-controller storm-control-policy
  Description: Configure FortiSwitch storm control policy to be applied on managed-switch
  ports.
  edit <name>
    set broadcast [enable|disable]
    set description {string}
    set rate {integer}
    set storm-control-mode [global|override|...]
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
  next
end
```

config switch-controller storm-control-policy

Parameter	Description	Type	Size								
broadcast	Enable/disable storm control to drop/allow broadcast traffic in override mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.</td></tr><tr><td><i>disable</i></td><td>Disable storm control for broadcast traffic to allow all packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.				
Option	Description										
<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.										
<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.										
description	Description of the storm control policy.	string	Maximum length: 63								
name	Storm control policy name.	string	Maximum length: 63								
rate	Threshold rate in packets per second at which storm traffic is controlled in override mode (default=500, 0 to drop all).	integer	Minimum value: 0 Maximum value: 10000000								
storm-control-mode	Set Storm control mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Apply Global or switch level storm control configuration.</td></tr><tr><td><i>override</i></td><td>Override global and switch level storm control to use port level configuration.</td></tr><tr><td><i>disabled</i></td><td>Disable storm control on the port entirely overriding global and switch level storm control.</td></tr></table>	Option	Description	<i>global</i>	Apply Global or switch level storm control configuration.	<i>override</i>	Override global and switch level storm control to use port level configuration.	<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.		
Option	Description										
<i>global</i>	Apply Global or switch level storm control configuration.										
<i>override</i>	Override global and switch level storm control to use port level configuration.										
<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.										

Parameter	Description	Type	Size
unknown-multicast	Enable/disable storm control to drop/allow unknown multicast traffic in override mode.	option	-

Option	Description
<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.
<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.

unknown-unicast	Enable/disable storm control to drop/allow unknown unicast traffic in override mode.	option	-

Option	Description
<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.
<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.

config switch-controller stp-instance



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.

```

config switch-controller stp-instance
    Description: Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.
    edit <id>
        set vlan-range <vlan-name1>, <vlan-name2>, ...
    next
end

```

config switch-controller stp-instance

Parameter	Description	Type	Size
id	Instance ID.	string	Maximum length: 2
vlan-range <vlan-name>	Configure VLAN range for STP instance. VLAN name.	string	Maximum length: 79

config switch-controller stp-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch spanning tree protocol (STP).

```

config switch-controller stp-settings
    Description: Configure FortiSwitch spanning tree protocol (STP).
    set forward-time {integer}

```

```

set hello-time {integer}
set max-age {integer}
set max-hops {integer}
set name {string}
set pending-timer {integer}
set revision {integer}
end

```

config switch-controller stp-settings

Parameter	Description	Type	Size
forward-time	Period of time a port is in listening and learning state (4 - 30 sec, default = 15).	integer	Minimum value: 4 Maximum value: 30
hello-time	Period of time between successive STP frame Bridge Protocol Data Units (BPDUs) sent on a port (1 - 10 sec, default = 2).	integer	Minimum value: 1 Maximum value: 10
max-age	Maximum time before a bridge port saves its configuration BPDU information (6 - 40 sec, default = 20).	integer	Minimum value: 6 Maximum value: 40
max-hops	Maximum number of hops between the root bridge and the furthest bridge (1- 40, default = 20).	integer	Minimum value: 1 Maximum value: 40
name	Name of global STP settings configuration.	string	Maximum length: 31
pending-timer	Pending time (1 - 15 sec, default = 4).	integer	Minimum value: 1 Maximum value: 15
revision	STP revision number (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535

config switch-controller switch-group



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

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
name	Switch group name.	string	Maximum length: 35

config switch-controller switch-interface-tag



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure switch object tags.

```
config switch-controller switch-interface-tag
    Description: Configure switch object tags.
    edit <name>
        next
    end
```

config switch-controller switch-interface-tag

Parameter	Description	Type	Size
name	Tag name.	string	Maximum length: 63

config switch-controller switch-log



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log).

```
config switch-controller switch-log
    Description: Configure FortiSwitch logging (logs are transferred to and inserted into
FortiGate event log).
    set severity [emergency|alert|...]
    set status [enable|disable]
end
```

config switch-controller switch-log

Parameter	Description	Type	Size
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-
Option	Description		
<i>emergency</i>	Emergency level.		
<i>alert</i>	Alert level.		
<i>critical</i>	Critical level.		

Parameter	Description	Type	Size

Option	Description
<i>error</i>	Error level.
<i>warning</i>	Warning level.
<i>notification</i>	Notification level.
<i>information</i>	Information level.
<i>debug</i>	Debug level.

status	Enable/disable adding FortiSwitch logs to FortiGate event log.	option	-

Option	Description
<i>enable</i>	Add FortiSwitch logs to FortiGate event log.
<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.

config switch-controller switch-profile



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch switch profile.


```
config switch-controller switch-profile
  Description: Configure FortiSwitch switch profile.
  edit <name>
    set login-passwd {password}
    set login-passwd-override [enable|disable]
  next
end
```

config switch-controller switch-profile

Parameter	Description	Type	Size						
login-passwd	Login password of managed FortiSwitch.	password	Not Specified						
login-passwd-override	Enable/disable overriding the admin administrator password for a managed FortiSwitch with the FortiGate admin administrator account password.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override a managed FortiSwitch's admin administrator password.</td></tr><tr><td><i>disable</i></td><td>Use the managed FortiSwitch admin administrator account password.</td></tr></table>			Option	Description	<i>enable</i>	Override a managed FortiSwitch's admin administrator password.	<i>disable</i>	Use the managed FortiSwitch admin administrator account password.
Option	Description								
<i>enable</i>	Override a managed FortiSwitch's admin administrator password.								
<i>disable</i>	Use the managed FortiSwitch admin administrator account password.								
name	FortiSwitch Profile name.	string	Maximum length: 35						

config switch-controller system



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure system-wide switch controller settings.

```
config switch-controller system
    Description: Configure system-wide switch controller settings.
    set data-sync-interval {integer}
    set parallel-process {integer}
    set parallel-process-override [disable|enable]
end
```

config switch-controller system

Parameter	Description	Type	Size
data-sync-interval	Time interval between collection of switch data (30 - 1800 sec, default = 60, 0 = disable).	integer	Minimum value: 30 Maximum value: 1800
parallel-process	Maximum number of parallel processes (1 - 300, default = 1).	integer	Minimum value: 1 Maximum value: 300

Parameter	Description	Type	Size
parallel-process-override	Enable/disable parallel process override.	option	-
Option	Description		
<i>disable</i>	Disable maximum parallel process override.		
<i>enable</i>	Enable maximum parallel process override.		

config switch-controller traffic-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch traffic policy.

```
config switch-controller traffic-policy
  Description: Configure FortiSwitch traffic policy.
  edit <name>
    set cos-queue {integer}
    set description {string}
    set guaranteed-bandwidth {integer}
    set guaranteed-burst {integer}
    set maximum-burst {integer}
    set policer-status [enable|disable]
```

```

        set type [ingress|egress]
    next
end

```

config switch-controller traffic-policy

Parameter	Description	Type	Size
cos-queue	COS queue(0 - 7), or unset to disable.	integer	Minimum value: 0 Maximum value: 7
description	Description of the traffic policy.	string	Maximum length: 63
guaranteed-bandwidth	Guaranteed bandwidth in kbps (max value = 524287000).	integer	Minimum value: 0 Maximum value: 524287000
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
name	Traffic policy name.	string	Maximum length: 63
policer-status	Enable/disable policer config on the traffic policy.	option	-

Option	Description
<i>enable</i>	Enable policer config on the traffic policy.
<i>disable</i>	Disable policer config on the traffic policy.

type	Configure type of policy(ingress/egress). Read-only.	option	-

Option	Description
<i>ingress</i>	Ingress policy.
<i>egress</i>	Egress policy.

config switch-controller traffic-sniffer



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.

```
config switch-controller traffic-sniffer
  Description: Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.
  set erspan-ip {ipv4-address}
  set mode [erspan-auto|rspan|...]
  config target-ip
    Description: Sniffer IPs to filter.
    edit <ip>
      set description {string}
    next
  end
  config target-mac
    Description: Sniffer MACs to filter.
    edit <mac>
      set description {string}
    next
  end
  config target-port
    Description: Sniffer ports to filter.
    edit <switch-id>
      set description {string}
      set in-ports <name1>, <name2>, ...
      set out-ports <name1>, <name2>, ...
    next
```

end
end

config switch-controller traffic-sniffer

Parameter	Description	Type	Size
erspan-ip	Configure ERSPAN collector IP address.	ipv4-address	Not Specified
mode	Configure traffic sniffer mode.	option	-
	Option	Description	
	<i>erspan-auto</i>	Mirror traffic using a GRE tunnel.	
	<i>rspan</i>	Mirror traffic on a layer2 VLAN.	
	<i>none</i>	Disable traffic mirroring (sniffer).	

config target-ip

Parameter	Description	Type	Size
description	Description for the sniffer IP.	string	Maximum length: 63
ip	Sniffer IP.	ipv4-address	Not Specified

config target-mac

Parameter	Description	Type	Size
description	Description for the sniffer MAC.	string	Maximum length: 63
mac	Sniffer MAC.	mac-address	Not Specified

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
switch-id	Managed-switch ID.	string	Maximum length: 16

config switch-controller virtual-port-pool



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

Configure virtual pool.

```
config switch-controller virtual-port-pool
    Description: Configure virtual pool.
    edit <name>
        set description {string}
    next
end
```

config switch-controller virtual-port-pool

Parameter	Description	Type	Size
description	Virtual switch pool description.	string	Maximum length: 63
name	Virtual switch pool name.	string	Maximum length: 35

system

This section includes syntax for the following commands:

- [config system 3g-modem custom on page 851](#)
- [config system accprofile on page 852](#)
- [config system admin on page 862](#)
- [config system affinity-interrupt on page 869](#)
- [config system affinity-packet-redistribution on page 870](#)
- [config system alarm on page 871](#)
- [config system alias on page 874](#)
- [config system api-user on page 875](#)
- [config system arp-table on page 876](#)
- [config system auto-install on page 890](#)
- [config system auto-script on page 891](#)
- [config system automation-action on page 877](#)
- [config system automation-destination on page 882](#)
- [config system automation-stitch on page 882](#)
- [config system automation-trigger on page 883](#)
- [config system autoupdate push-update on page 887](#)
- [config system autoupdate schedule on page 887](#)
- [config system autoupdate tunneling on page 888](#)
- [config system bypass on page 892](#)
- [config system central-management on page 894](#)
- [config system cluster-sync on page 899](#)
- [config system console on page 901](#)
- [config system csf on page 903](#)
- [config system custom-language on page 905](#)
- [config system ddns on page 906](#)
- [config system dedicated-mgmt on page 908](#)
- [config system dhcp6 server on page 920](#)
- [config system dhcp server on page 909](#)
- [config system dnp3-proxy on page 924](#)
- [config system dns-database on page 927](#)
- [config system dns-server on page 930](#)
- [config system dns on page 925](#)
- [config system dscp-based-priority on page 931](#)
- [config system elbc on page 932](#)
- [config system email-server on page 933](#)
- [config system external-resource on page 935](#)

-
- [config system fips-cc on page 937](#)
 - [config system fm on page 937](#)
 - [config system fortiguard on page 939](#)
 - [config system fortimanager on page 945](#)
 - [config system fortisandbox on page 946](#)
 - [config system fsso-polling on page 947](#)
 - [config system ftm-push on page 948](#)
 - [config system geneve on page 949](#)
 - [config system geoip-override on page 950](#)
 - [config system global on page 951](#)
 - [config system gre-tunnel on page 988](#)
 - [config system ha-monitor on page 1003](#)
 - [config system ha on page 990](#)
 - [config system interface on page 1003](#)
 - [config system ipip-tunnel on page 1052](#)
 - [config system ips-urlfilter-dns on page 1054](#)
 - [config system ips-urlfilter-dns6 on page 1055](#)
 - [config system ipsec-aggregate on page 1053](#)
 - [config system ipv6-neighbor-cache on page 1055](#)
 - [config system ipv6-tunnel on page 1056](#)
 - [config system isf-queue-profile on page 1057](#)
 - [config system link-monitor on page 1058](#)
 - [config system lldp network-policy on page 1061](#)
 - [config system lte-modem on page 1069](#)
 - [config system mac-address-table on page 1073](#)
 - [config system management-tunnel on page 1074](#)
 - [config system mobile-tunnel on page 1075](#)
 - [config system modem on page 1078](#)
 - [config system nat64 on page 1085](#)
 - [config system nd-proxy on page 1086](#)
 - [config system netflow on page 1087](#)
 - [config system network-visibility on page 1088](#)
 - [config system np6 on page 1090](#)
 - [config system np6xlite on page 1103](#)
 - [config system npu on page 1115](#)
 - [config system ntp on page 1127](#)
 - [config system object-tagging on page 1130](#)
 - [config system password-policy-guest-admin on page 1134](#)
 - [config system password-policy on page 1132](#)
 - [config system physical-switch on page 1136](#)
 - [config system pppoe-interface on page 1137](#)
 - [config system probe-response on page 1139](#)
 - [config system proxy-arp on page 1140](#)

-
- [config system ptp on page 1141](#)
 - [config system replacemsg-group on page 1156](#)
 - [config system replacemsg-image on page 1169](#)
 - [config system replacemsg admin on page 1142](#)
 - [config system replacemsg alertmail on page 1143](#)
 - [config system replacemsg auth on page 1144](#)
 - [config system replacemsg device-detection-portal on page 1145](#)
 - [config system replacemsg fortiguard-wf on page 1145](#)
 - [config system replacemsg ftp on page 1146](#)
 - [config system replacemsg http on page 1147](#)
 - [config system replacemsg icap on page 1148](#)
 - [config system replacemsg mail on page 1149](#)
 - [config system replacemsg nac-quar on page 1150](#)
 - [config system replacemsg nntp on page 1151](#)
 - [config system replacemsg spam on page 1151](#)
 - [config system replacemsg sslvpn on page 1152](#)
 - [config system replacemsg traffic-quota on page 1153](#)
 - [config system replacemsg utm on page 1154](#)
 - [config system replacemsg webproxy on page 1155](#)
 - [config system resource-limits on page 1169](#)
 - [config system saml on page 1172](#)
 - [config system sdn-connector on page 1175](#)
 - [config system session-helper on page 1181](#)
 - [config system session-ttl on page 1183](#)
 - [config system settings on page 1184](#)
 - [config system sflow on page 1203](#)
 - [config system sit-tunnel on page 1204](#)
 - [config system smc-ntp on page 1205](#)
 - [config system sms-server on page 1206](#)
 - [config system snmp community on page 1207](#)
 - [config system snmp sysinfo on page 1213](#)
 - [config system snmp user on page 1214](#)
 - [config system speed-test-server on page 1218](#)
 - [config system sso-admin on page 1219](#)
 - [config system storage on page 1220](#)
 - [config system stp on page 1222](#)
 - [config system switch-interface on page 1223](#)
 - [config system tos-based-priority on page 1225](#)
 - [config system vdom-dns on page 1227](#)
 - [config system vdom-exception on page 1228](#)
 - [config system vdom-link on page 1230](#)
 - [config system vdom-netflow on page 1231](#)
 - [config system vdom-property on page 1231](#)

- [config system vdom-radius-server on page 1233](#)
- [config system vdom-sflow on page 1234](#)
- [config system vdom on page 1226](#)
- [config system virtual-switch on page 1235](#)
- [config system virtual-wan-link on page 1237](#)
- [config system virtual-wire-pair on page 1253](#)
- [config system vxlan on page 1254](#)
- [config system wccp on page 1256](#)
- [config system wireless ap-status on page 1259](#)
- [config system wireless settings on page 1261](#)
- [config system zone on page 1264](#)

config system 3g-modem custom



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64, FortiGateRugged 35D.

3G MODEM custom.

```
config system 3g-modem custom
  Description: 3G MODEM custom.
  edit <id>
    set class-id {user}
    set init-string {string}
    set model {string}
    set modeswitch-string {string}
```

```

        set product-id {user}
        set vendor {string}
        set vendor-id {user}
    next
end

```

config system 3g-modem custom

Parameter	Description	Type	Size
class-id	USB interface class in hexadecimal format (00-ff).	user	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
init-string	Init string in hexadecimal format (even length).	string	Maximum length: 127
model	MODEM model name.	string	Maximum length: 35
modeswitch-string	Usb modeswitch arguments. e.g: '-v 1410 -p 9030 -V 1410 -P 9032 -u 3'	string	Maximum length: 127
product-id	USB product ID in hexadecimal format (0000-ffff).	user	Not Specified
vendor	MODEM vendor name.	string	Maximum length: 35
vendor-id	USB vendor ID in hexadecimal format (0000-ffff).	user	Not Specified

config system accprofile

Configure access profiles for system administrators.

```

config system accprofile
    Description: Configure access profiles for system administrators.
    edit <name>
        set admintimeout {integer}
        set admintimeout-override [enable|disable]
        set authgrp [none|read|...]
        set comments {var-string}
        set ftviewgrp [none|read|...]
        set fwgrp [none|read|...]
        config fwgrp-permission
            Description: Custom firewall permission.
            set address [none|read|...]
            set policy [none|read|...]
            set schedule [none|read|...]
            set service [none|read|...]
        end
    end
end

```

```

end
set loggrp [none|read|...]
config loggrp-permission
    Description: Custom Log & Report permission.
    set config [none|read|...]
    set data-access [none|read|...]
    set report-access [none|read|...]
    set threat-weight [none|read|...]
end
set netgrp [none|read|...]
config netgrp-permission
    Description: Custom network permission.
    set cfg [none|read|...]
    set packet-capture [none|read|...]
    set route-cfg [none|read|...]
end
set scope [vdom|global]
set secfabgrp [none|read|...]
set sysgrp [none|read|...]
config sysgrp-permission
    Description: Custom system permission.
    set admin [none|read|...]
    set cfg [none|read|...]
    set mnt [none|read|...]
    set upd [none|read|...]
end
set utmgrp [none|read|...]
config utmgrp-permission
    Description: Custom Security Profile permissions.
    set antivirus [none|read|...]
    set application-control [none|read|...]
    set data-loss-prevention [none|read|...]
    set dnsfilter [none|read|...]
    set emailfilter [none|read|...]
    set endpoint-control [none|read|...]
    set icap [none|read|...]
    set ips [none|read|...]
    set voip [none|read|...]
    set waf [none|read|...]
    set webfilter [none|read|...]
end
set vpngrp [none|read|...]
set wanoptgrp [none|read|...]
set wifi [none|read|...]
next
end

```

config system accprofile

Parameter	Description	Type	Size
admintimeout	Administrator timeout for this access profile (0 - 480 min, default = 10, 0 means never timeout).	integer	Minimum value: 1 Maximum value: 480
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-
	Option	Description	
	<i>enable</i>	Enable overriding the global administrator idle timeout.	
	<i>disable</i>	Disable overriding the global administrator idle timeout.	
authgrp	Administrator access to Users and Devices.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
comments	Comment.	var-string	Maximum length: 255
ftviewgrp	FortiView.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
fwgrp	Administrator access to the Firewall configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
	<i>custom</i>	Customized access.	
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
	<i>custom</i>	Customized access.	
name	Profile name.	string	Maximum length: 35
netgrp	Network Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
	<i>custom</i>	Customized access.	
scope	Scope of admin access: global or specific VDOM(s).	option	-
	Option	Description	
	<i>vdom</i>	VDOM access.	
	<i>global</i>	Global access.	
secfabgrp	Security Fabric.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
sysgrp	System Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
	<i>custom</i>	Customized access.	

Parameter	Description	Type	Size
utmgrp	Administrator access to Security Profiles.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
	<i>custom</i>	Customized access.	
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
wanoptgrp *	Administrator access to WAN Opt & Cache.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
wifi	Administrator access to the WiFi controller and Switch controller.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	

* This parameter may not exist in some models.

config fwgrp-permission

Parameter	Description	Type	Size
address	Address Configuration.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
policy	Policy Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
schedule	Schedule Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
service	Service Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	

config loggrp-permission

Parameter	Description	Type	Size
config	Log & Report configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
data-access	Log & Report Data Access.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
report-access	Log & Report Report Access.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
threat-weight	Log & Report Threat Weight.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	

config netgrp-permission

Parameter	Description	Type	Size
cfg	Network Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
packet-capture	Packet Capture Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
route-cfg	Router Configuration.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	

config sysgrp-permission

Parameter	Description	Type	Size
admin	Administrator Users.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
cfg	System Configuration.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
mnt	Maintenance.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	
upd	FortiGuard Updates.	option	-
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	

config utmgrp-permission

Parameter	Description	Type	Size								
antivirus	Antivirus profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
application-control	Application Control profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
data-loss-prevention	DLP profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
dnsfilter	DNS Filter profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
emailfilter	AntiSpam filter and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										

Parameter	Description	Type	Size								
endpoint-control	FortiClient Profiles.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
icap	ICAP profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
ips	IPS profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
voip	VoIP profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
waf	Web Application Firewall profiles and settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.		
Option	Description										
<i>none</i>	No access.										
<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.										
webfilter	Web Filter profiles and settings.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No access.	
	<i>read</i>	Read access.	
	<i>read-write</i>	Read/write access.	

config system admin

Configure admin users.

```
config system admin
  Description: Configure admin users.
  edit <name>
    set accprofile {string}
    set accprofile-override [enable|disable]
    set allow-remove-admin-session [enable|disable]
    set comments {var-string}
    set email-to {string}
    set force-password-change [enable|disable]
    set fortitoken {string}
    set guest-auth [disable|enable]
    set guest-lang {string}
    set guest-usergroups <name1>, <name2>, ...
    set ip6-trusthost1 {ipv6-prefix}
    set ip6-trusthost10 {ipv6-prefix}
    set ip6-trusthost2 {ipv6-prefix}
    set ip6-trusthost3 {ipv6-prefix}
    set ip6-trusthost4 {ipv6-prefix}
    set ip6-trusthost5 {ipv6-prefix}
    set ip6-trusthost6 {ipv6-prefix}
    set ip6-trusthost7 {ipv6-prefix}
    set ip6-trusthost8 {ipv6-prefix}
    set ip6-trusthost9 {ipv6-prefix}
    set password {password-2}
    set password-expire {user}
    set peer-auth [enable|disable]
    set peer-group {string}
    set radius-vdom-override [enable|disable]
    set remote-auth [enable|disable]
    set remote-group {string}
    set schedule {string}
    set sms-custom-server {string}
    set sms-phone {string}
    set sms-server [fortiguard|custom]
    set ssh-certificate {string}
    set ssh-public-key1 {user}
    set ssh-public-key2 {user}
    set ssh-public-key3 {user}
    set trusthost1 {ipv4-classnet}
    set trusthost10 {ipv4-classnet}
```

```

set trusthost2 {ipv4-classnet}
set trusthost3 {ipv4-classnet}
set trusthost4 {ipv4-classnet}
set trusthost5 {ipv4-classnet}
set trusthost6 {ipv4-classnet}
set trusthost7 {ipv4-classnet}
set trusthost8 {ipv4-classnet}
set trusthost9 {ipv4-classnet}
set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set vdom <name1>, <name2>, ...
set wildcard [enable|disable]

```

```
next
```

```
end
```

config system admin

Parameter	Description	Type	Size						
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiGate features.	string	Maximum length: 35						
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiGate features that this administrator can access.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable access profile override.</td></tr><tr><td><i>disable</i></td><td>Disable access profile override.</td></tr></table>			Option	Description	<i>enable</i>	Enable access profile override.	<i>disable</i>	Disable access profile override.
Option	Description								
<i>enable</i>	Enable access profile override.								
<i>disable</i>	Disable access profile override.								
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow-remove option.</td></tr><tr><td><i>disable</i></td><td>Disable allow-remove option.</td></tr></table>			Option	Description	<i>enable</i>	Enable allow-remove option.	<i>disable</i>	Disable allow-remove option.
Option	Description								
<i>enable</i>	Enable allow-remove option.								
<i>disable</i>	Disable allow-remove option.								
comments	Comment.	var-string	Maximum length: 255						
email-to	This administrator's email address.	string	Maximum length: 63						
force-password-change	Enable/disable force password change on next login.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable force password change on next login.</td></tr><tr><td><i>disable</i></td><td>Disable force password change on next login.</td></tr></table>	Option	Description	<i>enable</i>	Enable force password change on next login.	<i>disable</i>	Disable force password change on next login.		
	Option	Description							
	<i>enable</i>	Enable force password change on next login.							
<i>disable</i>	Disable force password change on next login.								
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16						
guest-auth	Enable/disable guest authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable guest authentication.</td></tr><tr><td><i>enable</i></td><td>Enable guest authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable guest authentication.	<i>enable</i>	Enable guest authentication.		
	Option	Description							
	<i>disable</i>	Disable guest authentication.							
<i>enable</i>	Enable guest authentication.								
guest-lang	Guest management portal language.	string	Maximum length: 35						
guest-usergroups <name>	Select guest user groups. Select guest user groups.	string	Maximum length: 79						
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified						
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						
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						
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						

Parameter	Description	Type	Size						
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						
name	User name.	string	Maximum length: 64						
password	Admin user password.	password-2	Not Specified						
password-expire	Password expire time.	user	Not Specified						
peer-auth	Set to enable peer certificate authentication (for HTTPS admin access).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable peer.</td></tr><tr><td><i>disable</i></td><td>Disable peer.</td></tr></table>	Option	Description	<i>enable</i>	Enable peer.	<i>disable</i>	Disable peer.		
Option	Description								
<i>enable</i>	Enable peer.								
<i>disable</i>	Disable peer.								
peer-group	Name of peer group defined under config user group which has PKI members. Used for peer certificate authentication (for HTTPS admin access).	string	Maximum length: 35						
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VDOM override.</td></tr><tr><td><i>disable</i></td><td>Disable VDOM override.</td></tr></table>	Option	Description	<i>enable</i>	Enable VDOM override.	<i>disable</i>	Disable VDOM override.		
Option	Description								
<i>enable</i>	Enable VDOM override.								
<i>disable</i>	Disable VDOM override.								
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable remote authentication.</td></tr><tr><td><i>disable</i></td><td>Disable remote authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable remote authentication.	<i>disable</i>	Disable remote authentication.		
Option	Description								
<i>enable</i>	Enable remote authentication.								
<i>disable</i>	Disable remote authentication.								
remote-group	User group name used for remote auth.	string	Maximum length: 35						

Parameter	Description	Type	Size						
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35						
sms-custom-server	Custom SMS server to send SMS messages to.	string	Maximum length: 35						
sms-phone	Phone number on which the administrator receives SMS messages.	string	Maximum length: 15						
sms-server	Send SMS messages using the FortiGuard SMS server or a custom server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>			Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.
	Option	Description							
	<i>fortiguard</i>	Send SMS by FortiGuard.							
<i>custom</i>	Send SMS by custom server.								
ssh-certificate	Select the certificate to be used by the FortiGate for authentication with an SSH client.	string	Maximum length: 35						
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified						
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified						
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified						
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified						
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						
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						

Parameter	Description	Type	Size
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
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
two-factor	Enable/disable two-factor authentication.	option	-

Option	Description
<i>disable</i>	Disable two-factor authentication.
<i>fortitoken</i>	Use FortiToken or FortiToken mobile two-factor authentication.
<i>fortitoken-cloud</i>	FortiToken Cloud Service.
<i>email</i>	Send a two-factor authentication code to the configured email-to email address.
<i>sms</i>	Send a two-factor authentication code to the configured sms-server and sms-phone.

Parameter	Description	Type	Size								
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortitoken</i></td><td>FortiToken authentication.</td></tr><tr><td><i>email</i></td><td>Email one time password.</td></tr><tr><td><i>sms</i></td><td>SMS one time password.</td></tr></table>	Option	Description	<i>fortitoken</i>	FortiToken authentication.	<i>email</i>	Email one time password.	<i>sms</i>	SMS one time password.		
Option	Description										
<i>fortitoken</i>	FortiToken authentication.										
<i>email</i>	Email one time password.										
<i>sms</i>	SMS one time password.										
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email</i></td><td>Email notification for activation code.</td></tr><tr><td><i>sms</i></td><td>SMS notification for activation code.</td></tr></table>	Option	Description	<i>email</i>	Email notification for activation code.	<i>sms</i>	SMS notification for activation code.				
Option	Description										
<i>email</i>	Email notification for activation code.										
<i>sms</i>	SMS notification for activation code.										
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79								
wildcard	Enable/disable wildcard RADIUS authentication.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username wildcard.</td></tr><tr><td><i>disable</i></td><td>Disable username wildcard.</td></tr></table>	Option	Description	<i>enable</i>	Enable username wildcard.	<i>disable</i>	Disable username wildcard.				
Option	Description										
<i>enable</i>	Enable username wildcard.										
<i>disable</i>	Disable username wildcard.										

config system affinity-interrupt



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

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure interrupt affinity.

```
config system affinity-interrupt
    Description: Configure interrupt affinity.
    edit <id>
        set affinity-cpumask {string}
        set interrupt {string}
    next
end
```

config system affinity-interrupt

Parameter	Description	Type	Size
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127
id	ID of the interrupt affinity setting.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
interrupt	Interrupt name.	string	Maximum length: 127

config system affinity-packet-redistribution



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

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure packet redistribution.

```
config system affinity-packet-redistribution
    Description: Configure packet redistribution.
    edit <id>
        set affinity-cpumask {string}
        set interface {string}
        set rxqid {integer}
    next
end
```

config system affinity-packet-redistribution

Parameter	Description	Type	Size
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127
id	ID of the packet redistribution setting.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Physical interface name on which to perform packet redistribution.	string	Maximum length: 127
rxqid	ID of the receive queue (when the interface has multiple queues) on which to perform packet redistribution.	integer	Minimum value: 0 Maximum value: 255

config system alarm

Configure alarm.

```
config system alarm
  Description: Configure alarm.
  set audible [enable|disable]
  config groups
    Description: Alarm groups.
    edit <id>
      set admin-auth-failure-threshold {integer}
      set admin-auth-lockout-threshold {integer}
      set decryption-failure-threshold {integer}
      set encryption-failure-threshold {integer}
      set fw-policy-id {integer}
      set fw-policy-id-threshold {integer}
      config fw-policy-violations
        Description: Firewall policy violations.
        edit <id>
          set dst-ip {ipv4-address}
          set dst-port {integer}
          set src-ip {ipv4-address}
          set src-port {integer}
          set threshold {integer}
        next
      end
      set log-full-warning-threshold {integer}
      set period {integer}
      set replay-attempt-threshold {integer}
      set self-test-failure-threshold {integer}
      set user-auth-failure-threshold {integer}
      set user-auth-lockout-threshold {integer}
```

```

        next
    end
    set status [enable|disable]
end

```

config system alarm

Parameter	Description	Type	Size
audible	Enable/disable audible alarm.	option	-
	Option	Description	
	<i>enable</i>	Enable audible alarm.	
	<i>disable</i>	Disable audible alarm.	
status	Enable/disable alarm.	option	-
	Option	Description	
	<i>enable</i>	Enable alarm.	
	<i>disable</i>	Disable alarm.	

config groups

Parameter	Description	Type	Size
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
decryption-failure-threshold	Decryption failure 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
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
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295
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
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

config fw-policy-violations

Parameter	Description	Type	Size
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535
id	Firewall policy violations ID.	integer	Minimum value: 0 Maximum value: 4294967295
src-ip	Source IP (0=all).	ipv4-address	Not Specified
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024

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
name	Alias command name.	string	Maximum length: 35

config system api-user

Configure API users.

```
config system api-user
  Description: Configure API users.
  edit <name>
    set accprofile {string}
    set api-key {password-2}
    set comments {var-string}
    set cors-allow-origin {string}
    set peer-auth [enable|disable]
    set peer-group {string}
    set schedule {string}
    config trusthost
      Description: Trusthost.
      edit <id>
        set ipv4-trusthost {ipv4-classnet}
        set ipv6-trusthost {ipv6-prefix}
        set type [ipv4-trusthost|ipv6-trusthost]
      next
    end
  set vdom <name1>, <name2>, ...
next
end
```

config system api-user

Parameter	Description	Type	Size
accprofile	Admin user access profile.	string	Maximum length: 35
api-key	Admin user password.	password-2	Not Specified
comments	Comment.	var-string	Maximum length: 255
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible.	string	Maximum length: 269
name	User name.	string	Maximum length: 35
peer-auth	Enable/disable peer authentication.	option	-

Option	Description

<i>enable</i>	Enable peer.

<i>disable</i>	Disable peer.

Parameter	Description	Type	Size
peer-group	Peer group name.	string	Maximum length: 35
schedule	Schedule name.	string	Maximum length: 35
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79

config trusthost

Parameter	Description	Type	Size
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified
type	Trusthost type.	option	-

Option	Description
<i>ipv4-trusthost</i>	IPv4 trusthost.
<i>ipv6-trusthost</i>	IPv6 trusthost.

config system arp-table

Configure ARP table.

```
config system arp-table
    Description: Configure ARP table.
    edit <id>
        set interface {string}
        set ip {ipv4-address}
        set mac {mac-address}
    next
end
```

config system arp-table

Parameter	Description	Type	Size
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Interface name.	string	Maximum length: 15
ip	IP address.	ipv4-address	Not Specified
mac	MAC address.	mac-address	Not Specified

config system automation-action

Action for automation stitches.

```
config system automation-action
  Description: Action for automation stitches.
  edit <name>
    set accprofile {string}
    set action-type [email|ios-notification|...]
    set alicloud-access-key-id {string}
    set alicloud-access-key-secret {password}
    set alicloud-account-id {string}
    set alicloud-function {string}
    set alicloud-function-authorization [anonymous|function]
    set alicloud-function-domain {string}
    set alicloud-region {string}
    set alicloud-service {string}
    set alicloud-version {string}
    set aws-api-id {string}
    set aws-api-key {password}
    set aws-api-path {string}
    set aws-api-stage {string}
    set aws-domain {string}
    set aws-region {string}
    set azure-api-key {password}
    set azure-app {string}
    set azure-domain {string}
    set azure-function {string}
    set azure-function-authorization [anonymous|function|...]
    set delay {integer}
    set email-body {string}
    set email-from {var-string}
    set email-subject {var-string}
    set email-to <name1>, <name2>, ...
    set gcp-function {string}
    set gcp-function-domain {string}
```

```

set gcp-function-region {string}
set gcp-project {string}
set headers <header1>, <header2>, ...
set http-body {var-string}
set method [post|put|...]
set minimum-interval {integer}
set port {integer}
set protocol [http|https]
set required [enable|disable]
set script {var-string}
set sdn-connector <name1>, <name2>, ...
set security-tag {string}
set tls-certificate {string}
set uri {var-string}
next
end

```

config system automation-action

Parameter	Description	Type	Size
accprofile	Access profile for CLI script action to access FortiGate features.	string	Maximum length: 35
action-type	Action type.	option	-

Option	Description
<i>email</i>	Send notification email.
<i>ios-notification</i>	Send push notification to FortiExplorer iOS.
<i>alert</i>	Generate FortiOS dashboard alert.
<i>disable-ssid</i>	Disable interface.
<i>quarantine</i>	Quarantine host.
<i>quarantine-forticlient</i>	Quarantine FortiClient by EMS.
<i>quarantine-nsx</i>	Quarantine NSX instance.
<i>ban-ip</i>	Ban IP address.
<i>aws-lambda</i>	Send log data to integrated AWS service.
<i>azure-function</i>	Send log data to an Azure function.
<i>google-cloud-function</i>	Send log data to a Google Cloud function.
<i>alicloud-function</i>	Send log data to an AliCloud function.
<i>webhook</i>	Send an HTTP request.
<i>cli-script</i>	Run CLI script.

Parameter	Description	Type	Size						
alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35						
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified						
alicloud-account-id	AliCloud account ID.	string	Maximum length: 63						
alicloud-function	AliCloud function name.	string	Maximum length: 128						
alicloud-function-authorization	AliCloud function authorization type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization (Authorization required).</td></tr></table>	Option	Description	<i>anonymous</i>	Anonymous authorization (No authorization required).	<i>function</i>	Function authorization (Authorization required).		
Option	Description								
<i>anonymous</i>	Anonymous authorization (No authorization required).								
<i>function</i>	Function authorization (Authorization required).								
alicloud-function-domain	AliCloud function domain.	string	Maximum length: 63						
alicloud-region	AliCloud region.	string	Maximum length: 63						
alicloud-service	AliCloud service name.	string	Maximum length: 128						
alicloud-version	AliCloud version.	string	Maximum length: 63						
aws-api-id	AWS API Gateway ID.	string	Maximum length: 35						
aws-api-key	AWS API Gateway API key.	password	Not Specified						
aws-api-path	AWS API Gateway path.	string	Maximum length: 63						
aws-api-stage	AWS API Gateway deployment stage name.	string	Maximum length: 63						
aws-domain	AWS domain.	string	Maximum length: 63						
aws-region	AWS region.	string	Maximum length: 35						
azure-api-key	Azure function API key.	password	Not Specified						

Parameter	Description	Type	Size								
azure-app	Azure function application name.	string	Maximum length: 63								
azure-domain	Azure function domain.	string	Maximum length: 63								
azure-function	Azure function name.	string	Maximum length: 63								
azure-function-authorization	Azure function authorization level.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization level (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization level (Function or Host Key required).</td></tr><tr><td><i>admin</i></td><td>Admin authorization level (Master Host Key required).</td></tr></table>	Option	Description	<i>anonymous</i>	Anonymous authorization level (No authorization required).	<i>function</i>	Function authorization level (Function or Host Key required).	<i>admin</i>	Admin authorization level (Master Host Key required).		
Option	Description										
<i>anonymous</i>	Anonymous authorization level (No authorization required).										
<i>function</i>	Function authorization level (Function or Host Key required).										
<i>admin</i>	Admin authorization level (Master Host Key required).										
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600								
email-body	Email body.	string	Maximum length: 1023								
email-from	Email sender name.	var-string	Maximum length: 127								
email-subject	Email subject.	var-string	Maximum length: 511								
email-to <name>	Email addresses. Email address.	string	Maximum length: 255								
gcp-function	Google Cloud function name.	string	Maximum length: 63								
gcp-function-domain	Google Cloud function domain.	string	Maximum length: 63								
gcp-function-region	Google Cloud function region.	string	Maximum length: 63								
gcp-project	Google Cloud Platform project name.	string	Maximum length: 63								
headers <header>	Request headers. Request header.	string	Maximum length: 255								
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 1023								

Parameter	Description	Type	Size												
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>post</i></td><td>POST.</td></tr><tr><td><i>put</i></td><td>PUT.</td></tr><tr><td><i>get</i></td><td>GET.</td></tr><tr><td><i>patch</i></td><td>PATCH.</td></tr><tr><td><i>delete</i></td><td>DELETE.</td></tr></table>	Option	Description	<i>post</i>	POST.	<i>put</i>	PUT.	<i>get</i>	GET.	<i>patch</i>	PATCH.	<i>delete</i>	DELETE.		
	Option	Description													
	<i>post</i>	POST.													
	<i>put</i>	PUT.													
	<i>get</i>	GET.													
	<i>patch</i>	PATCH.													
	<i>delete</i>	DELETE.													
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000												
name	Name.	string	Maximum length: 64												
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535												
protocol	Request protocol.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.								
	Option	Description													
	<i>http</i>	HTTP.													
<i>https</i>	HTTPS.														
required	Required in action chain.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Required in action chain.</td></tr><tr><td><i>disable</i></td><td>Not required in action chain.</td></tr></table>	Option	Description	<i>enable</i>	Required in action chain.	<i>disable</i>	Not required in action chain.								
	Option	Description													
	<i>enable</i>	Required in action chain.													
<i>disable</i>	Not required in action chain.														
script	CLI script.	var-string	Maximum length: 1023												
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79												
security-tag	NSX security tag.	string	Maximum length: 255												

Parameter	Description	Type	Size
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35
uri	Request API URI.	var-string	Maximum length: 1023

config system automation-destination

Automation destinations.

```
config system automation-destination
  Description: Automation destinations.
  edit <name>
    set destination <name1>, <name2>, ...
    set ha-group-id {integer}
    set type [fortigate|ha-cluster]
  next
end
```

config system automation-destination

Parameter	Description	Type	Size
destination <name>	Destinations. Destination.	string	Maximum length: 31
ha-group-id	Cluster group ID set for this destination (default = 0).	integer	Minimum value: 0 Maximum value: 255
name	Name.	string	Maximum length: 35
type	Destination type.	option	-

Option	Description
<i>fortigate</i>	FortiGate set as destination.
<i>ha-cluster</i>	HA cluster set as destination.

config system automation-stitch

Automation stitches.

```
config system automation-stitch
  Description: Automation stitches.
```

```

edit <name>
    set action <name1>, <name2>, ...
    set destination <name1>, <name2>, ...
    set status [enable|disable]
    set trigger {string}
next
end

```

config system automation-stitch

Parameter	Description	Type	Size						
action <name>	Action names. Action name.	string	Maximum length: 79						
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79						
name	Name.	string	Maximum length: 35						
status	Enable/disable this stitch.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stitch.</td></tr><tr><td><i>disable</i></td><td>Disable stitch.</td></tr></table>		Option	Description	<i>enable</i>	Enable stitch.	<i>disable</i>	Disable stitch.	
	Option	Description							
	<i>enable</i>	Enable stitch.							
<i>disable</i>	Disable stitch.								
trigger	Trigger name.	string	Maximum length: 35						

config system automation-trigger

Trigger for automation stitches.

```

config system automation-trigger
    Description: Trigger for automation stitches.
    edit <name>
        set event-type [ioc|event-log|...]
        set faz-event-name {var-string}
        set faz-event-severity {var-string}
        set faz-event-tags {var-string}
        config fields
            Description: Customized trigger field settings.
            edit <id>
                set name {string}
                set value {var-string}
            next
        end
        set ioc-level [medium|high]
        set license-type [forticare-support|fortiguard-webfilter|...]
        set logid {integer}
    end
end

```

```

        set trigger-day {integer}
        set trigger-frequency [hourly|daily|...]
        set trigger-hour {integer}
        set trigger-minute {integer}
        set trigger-type [event-based|scheduled]
        set trigger-weekday [sunday|monday|...]
    next
end

```

config system automation-trigger

Parameter	Description	Type	Size
event-type	Event type.	option	-
	Option	Description	
	<i>ioc</i>	Indicator of compromise detected.	
	<i>event-log</i>	Use log ID as trigger.	
	<i>reboot</i>	Device reboot.	
	<i>low-memory</i>	Conserve mode due to low memory.	
	<i>high-cpu</i>	High CPU usage.	
	<i>license-near-expiry</i>	License near expiration date.	
	<i>ha-failover</i>	HA failover.	
	<i>config-change</i>	Configuration change.	
	<i>security-rating-summary</i>	Security rating summary.	
	<i>virus-ips-db-updated</i>	Virus and IPS database updated.	
	<i>faz-event</i>	FortiAnalyzer event.	
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
ioc-level	IOC threat level.	option	-

Parameter	Description	Type	Size																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>medium</i></td><td>IOC level medium and high.</td></tr><tr><td><i>high</i></td><td>IOC level high only.</td></tr></table>	Option	Description	<i>medium</i>	IOC level medium and high.	<i>high</i>	IOC level high only.												
	Option	Description																	
	<i>medium</i>	IOC level medium and high.																	
<i>high</i>	IOC level high only.																		
license-type	License type.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forticare-support</i></td><td>FortiCare support license.</td></tr><tr><td><i>fortiguard-webfilter</i></td><td>FortiGuard web filter license.</td></tr><tr><td><i>fortiguard-antispam</i></td><td>FortiGuard antispam license.</td></tr><tr><td><i>fortiguard-antivirus</i></td><td>FortiGuard AntiVirus license.</td></tr><tr><td><i>fortiguard-ips</i></td><td>FortiGuard IPS license.</td></tr><tr><td><i>fortiguard-management</i></td><td>FortiGuard management service license.</td></tr><tr><td><i>forticloud</i></td><td>FortiCloud license.</td></tr></table>	Option	Description	<i>forticare-support</i>	FortiCare support license.	<i>fortiguard-webfilter</i>	FortiGuard web filter license.	<i>fortiguard-antispam</i>	FortiGuard antispam license.	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.	<i>fortiguard-ips</i>	FortiGuard IPS license.	<i>fortiguard-management</i>	FortiGuard management service license.	<i>forticloud</i>	FortiCloud license.		
	Option	Description																	
	<i>forticare-support</i>	FortiCare support license.																	
	<i>fortiguard-webfilter</i>	FortiGuard web filter license.																	
	<i>fortiguard-antispam</i>	FortiGuard antispam license.																	
	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.																	
	<i>fortiguard-ips</i>	FortiGuard IPS license.																	
<i>fortiguard-management</i>	FortiGuard management service license.																		
<i>forticloud</i>	FortiCloud license.																		
logid	Log ID to trigger event.	integer	Minimum value: 1 Maximum value: 65535																
name	Name.	string	Maximum length: 35																
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31																
trigger-frequency	Scheduled trigger frequency (default = daily).	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hourly</i></td><td>Run hourly.</td></tr><tr><td><i>daily</i></td><td>Run daily.</td></tr><tr><td><i>weekly</i></td><td>Run weekly.</td></tr><tr><td><i>monthly</i></td><td>Run monthly.</td></tr></table>	Option	Description	<i>hourly</i>	Run hourly.	<i>daily</i>	Run daily.	<i>weekly</i>	Run weekly.	<i>monthly</i>	Run monthly.								
	Option	Description																	
	<i>hourly</i>	Run hourly.																	
	<i>daily</i>	Run daily.																	
<i>weekly</i>	Run weekly.																		
<i>monthly</i>	Run monthly.																		

Parameter	Description	Type	Size																
trigger-hour	Hour of the day on which to trigger (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23																
trigger-minute	Minute of the hour on which to trigger (0 - 59, default = 0).	integer	Minimum value: 0 Maximum value: 59																
trigger-type	Trigger type.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event-based</i></td><td>Event based trigger.</td></tr><tr><td><i>scheduled</i></td><td>Scheduled trigger.</td></tr></table>			Option	Description	<i>event-based</i>	Event based trigger.	<i>scheduled</i>	Scheduled trigger.										
Option	Description																		
<i>event-based</i>	Event based trigger.																		
<i>scheduled</i>	Scheduled trigger.																		
trigger-weekday	Day of week for trigger.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>			Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.
Option	Description																		
<i>sunday</i>	Sunday.																		
<i>monday</i>	Monday.																		
<i>tuesday</i>	Tuesday.																		
<i>wednesday</i>	Wednesday.																		
<i>thursday</i>	Thursday.																		
<i>friday</i>	Friday.																		
<i>saturday</i>	Saturday.																		

config fields

Parameter	Description	Type	Size
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Name.	string	Maximum length: 35
value	Value.	var-string	Maximum length: 63

config system autoupdate push-update

Configure push updates.

```
config system autoupdate push-update
  Description: Configure push updates.
  set address {string}
  set override [enable|disable]
  set port {integer}
  set status [enable|disable]
end
```

config system autoupdate push-update

Parameter	Description	Type	Size
address	IPv4 or IPv6 address used by FortiGuard servers to send push updates to this FortiGate.	string	Maximum length: 63
override	Enable/disable push update override server.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
port	Push update override port. (Do not overlap with other service ports)	integer	Minimum value: 0 Maximum value: 65535
status	Enable/disable push updates.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config system autoupdate schedule

Configure update schedule.

```
config system autoupdate schedule
  Description: Configure update schedule.
  set day [Sunday|Monday|...]
  set frequency [every|daily|...]
  set status [enable|disable]
```

```

    set time {user}
end

```

config system autoupdate schedule

Parameter	Description	Type	Size
day	Update day.	option	-
	Option	Description	
	<i>Sunday</i>	Update every Sunday.	
	<i>Monday</i>	Update every Monday.	
	<i>Tuesday</i>	Update every Tuesday.	
	<i>Wednesday</i>	Update every Wednesday.	
	<i>Thursday</i>	Update every Thursday.	
	<i>Friday</i>	Update every Friday.	
	<i>Saturday</i>	Update every Saturday.	
frequency	Update frequency.	option	-
	Option	Description	
	<i>every</i>	Time interval.	
	<i>daily</i>	Every day.	
	<i>weekly</i>	Every week.	
status	Enable/disable scheduled updates.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
time	Update time.	user	Not Specified

config system autoupdate tunneling

Configure web proxy tunnelling for the FDN.

```

config system autoupdate tunneling
    Description: Configure web proxy tunnelling for the FDN.
    set address {string}
    set password {password}
    set port {integer}
    set status [enable|disable]

```



```
set username {string}
end
```

config system autoupdate tunneling

Parameter	Description	Type	Size						
address	Web proxy IP address or FQDN.	string	Maximum length: 63						
password	Web proxy password.	password	Not Specified						
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535						
status	Enable/disable web proxy tunnelling.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
username	Web proxy username.	string	Maximum length: 49						

config system auto-install



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGateRugged 35D.

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable config.</td></tr><tr><td><i>disable</i></td><td>Disable config.</td></tr></table>			Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.
Option	Description								
<i>enable</i>	Enable config.								
<i>disable</i>	Disable config.								

Parameter	Description	Type	Size
auto-install-image	Enable/disable auto install the image in USB disk.	option	-
	Option	Description	
	<i>enable</i>	Enable config.	
	<i>disable</i>	Disable config.	
default-config-file	Default config file name in USB disk.	string	Maximum length: 127
default-image-file	Default image file name in USB disk.	string	Maximum length: 127

config system auto-script

Configure auto script.

```
config system auto-script
    Description: Configure auto script.
    edit <name>
        set interval {integer}
        set output-size {integer}
        set repeat {integer}
        set script {var-string}
        set start [manual|auto]
    next
end
```

config system auto-script

Parameter	Description	Type	Size
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600
name	Auto script name.	string	Maximum length: 35
output-size	Number of megabytes to limit script output to (10 - 1024, default = 10).	integer	Minimum value: 10 Maximum value: 1024

Parameter	Description	Type	Size
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535
script	List of FortiOS CLI commands to repeat.	var-string	Maximum length: 1023
start	Script starting mode.	option	-

Option	Description
<i>manual</i>	Starting manually.
<i>auto</i>	Starting automatically.

config system bypass



This command is available for model(s): FortiGate 2500E, FortiGate 400E Bypass, FortiGate 800D, FortiGate 80F Bypass, FortiGateRugged 60F 3G4G, FortiGateRugged 60F.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure system bypass.

```
config system bypass
  Description: Configure system bypass.
  set auto-recover [enable|disable]
  set bypass-timeout [2|4|...]
```

```

set bypass-watchdog [enable|disable]
set poweroff-bypass [enable|disable]
end

```

config system bypass

Parameter	Description	Type	Size
auto-recover *	Automatically recover from bypass mode after system reboot.	option	-
	Option	Description	
	<i>enable</i>	Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.	
	<i>disable</i>	Keep interfaces in bypass mode if bypass was previously triggered.	
bypass-timeout *	timeout setting for bypass watchdog	option	-
	Option	Description	
	2	2 second	
	4	4 second	
	6	6 second	
	8	8 second	
	10	10 second	
	12	12 second	
	14	14 second	
bypass-watchdog	watchdog to bypass interfaces in case of software/hardware failure	option	-
	Option	Description	
	<i>enable</i>	Enable watchdog for bypass interfaces.	
	<i>disable</i>	Disable watchdog for bypass interfaces.	
poweroff-bypass *	set interface bypass state in power off	option	-
	Option	Description	
	<i>enable</i>	Enable bypass when power off.	
	<i>disable</i>	Disable bypass when power off.	

* This parameter may not exist in some models.

config system central-management

Configure central management.

```
config system central-management
    Description: Configure central management.
    set allow-monitor [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set allow-remote-firmware-upgrade [enable|disable]
    set allow-remote-lte-firmware-upgrade [enable|disable]
    set ca-cert {user}
    set enc-algorithm [default|high|...]
    set fmg {user}
    set fmg-source-ip {ipv4-address}
    set fmg-source-ip6 {ipv6-address}
    set fmg-update-port [8890|443]
    set include-default-servers [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set local-cert {string}
    set ltefw-upgrade-frequency [everyHour|every12hour|...]
    set ltefw-upgrade-time {string}
    set mode [normal|backup]
    set schedule-config-restore [enable|disable]
    set schedule-script-restore [enable|disable]
    set serial-number {user}
    config server-list
        Description: Additional servers that the FortiGate can use for updates (for AV, IPS,
updates) and ratings (for web filter and antispam ratings) servers.
        edit <id>
            set addr-type [ipv4|ipv6|...]
            set fqdn {string}
            set server-address {ipv4-address}
            set server-address6 {ipv6-address}
            set server-type {option1}, {option2}, ...
        next
    end
    set type [fortimanager|fortiguard|...]
    set use-elbc-vdom [enable|disable]
    set vdom {string}
end
```

config system central-management

Parameter	Description	Type	Size
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiGate	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable remote monitoring of device.	
	<i>disable</i>	Disable remote monitoring of device.	
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiGate.	option	-
	Option	Description	
	<i>enable</i>	Enable push configuration.	
	<i>disable</i>	Disable push configuration.	
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiGate.	option	-
	Option	Description	
	<i>enable</i>	Enable push firmware.	
	<i>disable</i>	Disable push firmware.	
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiGate from the central management server.	option	-
	Option	Description	
	<i>enable</i>	Enable remote firmware upgrade.	
	<i>disable</i>	Disable remote firmware upgrade.	
allow-remote-lte-firmware-upgrade *	Enable/disable remotely upgrading the lte firmware on this FortiGate from the central management server.	option	-
	Option	Description	
	<i>enable</i>	Enable remote lte firmware upgrade.	
	<i>disable</i>	Disable remote lte firmware upgrade.	
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified
enc-algorithm	Encryption strength for communications between the FortiGate and central management.	option	-

Parameter	Description	Type	Size

Option	Description
<i>default</i>	High strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD.
<i>high</i>	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.
<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CBC-SHA, DES-CBC-SHA, DES-CBC-MD5.

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
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-

Option	Description
<i>8890</i>	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.
<i>443</i>	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.

include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-

Option	Description
<i>enable</i>	Enable inclusion of public FortiGuard servers in the override server list.
<i>disable</i>	Disable inclusion of public FortiGuard servers in the override server list.

interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-

Option	Description
<i>auto</i>	Set outgoing interface automatically.
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.
<i>specify</i>	Set outgoing interface manually.

Parameter	Description	Type	Size										
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35										
ltefw-upgrade-frequency *	Set LTE firmware auto pushdown frequency.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>everyHour</i></td><td>Auto check and pushdown LTE firmware every hour</td></tr><tr><td><i>every12hour</i></td><td>Auto check and pushdown LTE firmware every 12 hours</td></tr><tr><td><i>everyDay</i></td><td>Auto check and pushdown LTE firmware every day</td></tr><tr><td><i>everyWeek</i></td><td>Auto check and pushdown LTE firmware every week</td></tr></table>	Option	Description	<i>everyHour</i>	Auto check and pushdown LTE firmware every hour	<i>every12hour</i>	Auto check and pushdown LTE firmware every 12 hours	<i>everyDay</i>	Auto check and pushdown LTE firmware every day	<i>everyWeek</i>	Auto check and pushdown LTE firmware every week		
Option	Description												
<i>everyHour</i>	Auto check and pushdown LTE firmware every hour												
<i>every12hour</i>	Auto check and pushdown LTE firmware every 12 hours												
<i>everyDay</i>	Auto check and pushdown LTE firmware every day												
<i>everyWeek</i>	Auto check and pushdown LTE firmware every week												
ltefw-upgrade-time *	Schedule next LTE firmware upgrade time (Local Time). Format: YYYY-MM-DD HH:MM:SS	string	Maximum length: 35										
mode	Central management mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Manage and configure this FortiGate from FortiManager.</td></tr><tr><td><i>backup</i></td><td>Manage and configure this FortiGate locally and back up its config FortiManager.</td></tr></table>	Option	Description	<i>normal</i>	Manage and configure this FortiGate from FortiManager.	<i>backup</i>	Manage and configure this FortiGate locally and back up its config FortiManager.						
Option	Description												
<i>normal</i>	Manage and configure this FortiGate from FortiManager.												
<i>backup</i>	Manage and configure this FortiGate locally and back up its config FortiManager.												
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiGate.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable scheduled configuration restore.</td></tr><tr><td><i>disable</i></td><td>Disable scheduled configuration restore.</td></tr></table>	Option	Description	<i>enable</i>	Enable scheduled configuration restore.	<i>disable</i>	Disable scheduled configuration restore.						
Option	Description												
<i>enable</i>	Enable scheduled configuration restore.												
<i>disable</i>	Disable scheduled configuration restore.												
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiGate.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable scheduled script restore.</td></tr><tr><td><i>disable</i></td><td>Disable scheduled script restore.</td></tr></table>	Option	Description	<i>enable</i>	Enable scheduled script restore.	<i>disable</i>	Disable scheduled script restore.						
Option	Description												
<i>enable</i>	Enable scheduled script restore.												
<i>disable</i>	Disable scheduled script restore.												
serial-number	Serial number.	user	Not Specified										
type	Central management type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortimanager</i></td><td>FortiManager.</td></tr></table>	Option	Description	<i>fortimanager</i>	FortiManager.								
Option	Description												
<i>fortimanager</i>	FortiManager.												

Parameter	Description	Type	Size
	Option	Description	
	<i>fortiguard</i>	Central management of this FortiGate using FortiCloud.	
	<i>none</i>	No central management.	
use-elbc-vdom *	Enable/disable use of special ELBC config sync VDOM to connect to FortiManager.	option	-
	Option	Description	
	<i>enable</i>	enable	
	<i>disable</i>	disable	
vdom	Virtual domain (VDOM) name to use when communicating with FortiManager.	string	Maximum length: 31

* This parameter may not exist in some models.

config server-list

Parameter	Description	Type	Size								
addr-type	Indicate whether the FortiGate communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 address.</td></tr><tr><td>ipv6</td><td>IPv6 address.</td></tr><tr><td>fqdn</td><td>FQDN.</td></tr></table>			Option	Description	ipv4	IPv4 address.	ipv6	IPv6 address.	fqdn	FQDN.
	Option	Description									
	ipv4	IPv4 address.									
	ipv6	IPv6 address.									
	fqdn	FQDN.									
fqdn	FQDN address of override server.	string	Maximum length: 255								
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295								
server-address	IPv4 address of override server.	ipv4-address	Not Specified								
server-address6	IPv6 address of override server.	ipv6-address	Not Specified								
server-type	FortiGuard service type.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>update</i>	AV, IPS, and AV-query update server.	
	<i>rating</i>	Web filter and anti-spam rating server.	

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 down-intfs-before-sess-sync <name1>, <name2>, ...
        set hb-interval {integer}
        set hb-lost-threshold {integer}
        set ipsec-tunnel-sync [enable|disable]
        set peerip {ipv4-address}
        set peervd {string}
        config session-sync-filter
            Description: Add one or more filters if you only want to synchronize some
sessions. Use the filter to configure the types of sessions to synchronize.
            config custom-service
                Description: Only sessions using these custom services are synchronized. Use
source and destination port ranges to define these custome services.
                edit <id>
                    set dst-port-range {user}
                    set src-port-range {user}
                next
            end
            set dstaddr {ipv4-classnet-any}
            set dstaddr6 {ipv6-network}
            set dstintf {string}
            set srcaddr {ipv4-classnet-any}
            set srcaddr6 {ipv6-network}
            set srcintf {string}
        end
        set slave-add-ike-routes [enable|disable]
        set syncvd <name1>, <name2>, ...
    next
end
```

config system cluster-sync

Parameter	Description	Type	Size						
down-intfs-before-sess-sync <name>	List of interfaces to be turned down before session synchronization is complete. Interface name.	string	Maximum length: 79						
hb-interval	Heartbeat interval (1 - 10 sec).	integer	Minimum value: 1 Maximum value: 10						
hb-lost-threshold	Lost heartbeat threshold (1 - 10).	integer	Minimum value: 1 Maximum value: 10						
ipsec-tunnel-sync	Enable/disable IPsec tunnel synchronization.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec tunnel synchronization.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec tunnel synchronization.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec tunnel synchronization.	<i>disable</i>	Disable IPsec tunnel synchronization.		
Option	Description								
<i>enable</i>	Enable IPsec tunnel synchronization.								
<i>disable</i>	Disable IPsec tunnel synchronization.								
peerip	IP address of the interface on the peer unit that is used for the session synchronization link.	ipv4-address	Not Specified						
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						
slave-add-ike-routes	Enable/disable IKE route announcement on the backup unit.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add IKE routes to the backup unit.</td></tr><tr><td><i>disable</i></td><td>Do not add IKE routes to the backup unit.</td></tr></table>	Option	Description	<i>enable</i>	Add IKE routes to the backup unit.	<i>disable</i>	Do not add IKE routes to the backup unit.		
Option	Description								
<i>enable</i>	Add IKE routes to the backup unit.								
<i>disable</i>	Do not add IKE routes to the backup unit.								
sync-id	Sync ID.	integer	Minimum value: 0 Maximum value: 4294967295						
syncvd <name>	Sessions from these VDOMs are synchronized using this session synchronization configuration. VDOM name.	string	Maximum length: 79						

config session-sync-filter

Parameter	Description	Type	Size
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
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
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
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
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

config custom-service

Parameter	Description	Type	Size
dst-port-range	Custom service destination port range.	user	Not Specified
id	Custom service ID.	integer	Minimum value: 0 Maximum value: 4294967295
src-port-range	Custom service source port range.	user	Not Specified

config system console

Configure console.

```
config system console
  Description: Configure console.
  set baudrate [9600|19200|...]
  set fortiexplorer [enable|disable]
  set login [enable|disable]
  set mode [batch|line]
```

```

set output [standard|more]
end

```

config system console

Parameter	Description	Type	Size												
baudrate	Console baud rate.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>9600</td><td>9600</td></tr><tr><td>19200</td><td>19200</td></tr><tr><td>38400</td><td>38400</td></tr><tr><td>57600</td><td>57600</td></tr><tr><td>115200</td><td>115200</td></tr></table>	Option	Description	9600	9600	19200	19200	38400	38400	57600	57600	115200	115200		
Option	Description														
9600	9600														
19200	19200														
38400	38400														
57600	57600														
115200	115200														
fortiexplorer *	Enable/disable access for FortiExplorer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiExplorer access.</td></tr><tr><td>disable</td><td>Disable FortiExplorer access.</td></tr></table>	Option	Description	enable	Enable FortiExplorer access.	disable	Disable FortiExplorer access.								
Option	Description														
enable	Enable FortiExplorer access.														
disable	Disable FortiExplorer access.														
login	Enable/disable serial console and FortiExplorer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Console login enable.</td></tr><tr><td>disable</td><td>Console login disable.</td></tr></table>	Option	Description	enable	Console login enable.	disable	Console login disable.								
Option	Description														
enable	Console login enable.														
disable	Console login disable.														
mode	Console mode.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>batch</td><td>Batch mode.</td></tr><tr><td>line</td><td>Line mode.</td></tr></table>	Option	Description	batch	Batch mode.	line	Line mode.								
Option	Description														
batch	Batch mode.														
line	Line mode.														
output	Console output mode.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>standard</td><td>Standard output.</td></tr><tr><td>more</td><td>More page output.</td></tr></table>	Option	Description	standard	Standard output.	more	More page output.								
Option	Description														
standard	Standard output.														
more	More page output.														

* This parameter may not exist in some models.

config system csf

Add this FortiGate to a Security Fabric or set up a new Security Fabric on this FortiGate.

```
config system csf
    Description: Add this FortiGate to a Security Fabric or set up a new Security Fabric on
this FortiGate.
    set configuration-sync [default|local]
    config fabric-device
        Description: Fabric device configuration.
        edit <name>
            set access-token {varlen_password}
            set device-ip {ipv4-address}
            set https-port {integer}
        next
    end
    set group-name {string}
    set group-password {password}
    set management-ip {string}
    set management-port {integer}
    set status [enable|disable]
    config trusted-list
        Description: Pre-authorized and blocked security fabric nodes.
        edit <serial>
            set action [accept|deny]
            set downstream-authorization [enable|disable]
            set ha-members {string}
        next
    end
    set upstream-ip {ipv4-address}
    set upstream-port {integer}
end
```

config system csf

Parameter	Description	Type	Size
configuration-sync	Configuration sync mode.	option	-
	Option	Description	
	<i>default</i>	Synchronize configuration for FortiAnalyzer, FortiSandbox and Central Management to root node.	
	<i>local</i>	Do not synchronize configuration with root node.	
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

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						
status	Enable/disable Security Fabric.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Security Fabric.</td></tr><tr><td><i>disable</i></td><td>Disable Security Fabric.</td></tr></table>			Option	Description	<i>enable</i>	Enable Security Fabric.	<i>disable</i>	Disable Security Fabric.
Option	Description								
<i>enable</i>	Enable Security Fabric.								
<i>disable</i>	Disable Security Fabric.								
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 (default = 8013).	integer	Minimum value: 1 Maximum value: 65535						

config fabric-device

Parameter	Description	Type	Size
access-token	Device access token.	varlen_ password	Not Specified
device-ip	Device IP.	ipv4-address	Not Specified
https-port	HTTPS port for fabric device.	integer	Minimum value: 1 Maximum value: 65535
name	Device name.	string	Maximum length: 35

config trusted-list

Parameter	Description	Type	Size
action	Security fabric authorization action.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>accept</i>	Accept authorization request.	
	<i>deny</i>	Deny authorization request.	
downstream-authorization	Trust authorizations by this node's administrator.	option	-
	Option	Description	
	<i>enable</i>	Enable downstream authorization.	
	<i>disable</i>	Disable downstream authorization.	
ha-members	HA members.	string	Maximum length: 19
serial	Serial.	string	Maximum length: 19

config system custom-language

Configure custom languages.

```
config system custom-language
    Description: Configure custom languages.
    edit <name>
        set comments {var-string}
        set filename {string}
    next
end
```

config system custom-language

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 255
filename	Custom language file path.	string	Maximum length: 63
name	Name.	string	Maximum length: 35

config system ddns

Configure DDNS.

```
config system ddns
  Description: Configure DDNS.
  edit <ddnsid>
    set bound-ip {ipv4-address}
    set clear-text [disable|enable]
    set ddns-auth [disable|tsig]
    set ddns-domain {string}
    set ddns-key {user}
    set ddns-keyname {string}
    set ddns-password {password}
    set ddns-server [dyndns.org|dyns.net|...]
    set ddns-server-ip {ipv4-address}
    set ddns-sn {string}
    set ddns-ttl {integer}
    set ddns-username {string}
    set ddns-zone {string}
    set monitor-interface <interface-name1>, <interface-name2>, ...
    set ssl-certificate {string}
    set update-interval {integer}
    set use-public-ip [disable|enable]
  next
end
```

config system ddns

Parameter	Description	Type	Size						
bound-ip	Bound IP address. Read-only.	ipv4-address	Not Specified						
clear-text	Enable/disable use of clear text connections.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of clear text connections.</td></tr><tr><td><i>enable</i></td><td>Enable use of clear text connections.</td></tr></table>			Option	Description	<i>disable</i>	Disable use of clear text connections.	<i>enable</i>	Enable use of clear text connections.
	Option	Description							
	<i>disable</i>	Disable use of clear text connections.							
<i>enable</i>	Enable use of clear text connections.								
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DDNS authentication.</td></tr><tr><td><i>tsig</i></td><td>Enable TSIG authentication based on RFC2845.</td></tr></table>			Option	Description	<i>disable</i>	Disable DDNS authentication.	<i>tsig</i>	Enable TSIG authentication based on RFC2845.
	Option	Description							
	<i>disable</i>	Disable DDNS authentication.							
<i>tsig</i>	Enable TSIG authentication based on RFC2845.								
ddns-domain	Your fully qualified domain name (for example, yourname.DDNS.com).	string	Maximum length: 64						

Parameter	Description	Type	Size
ddns-key	DDNS update key (base 64 encoding).	user	Not Specified
ddns-keyname	DDNS update key name.	string	Maximum length: 64
ddns-password	DDNS password.	password	Not Specified
ddns-server	Select a DDNS service provider.	option	-

Option	Description
<i>dyndns.org</i>	members.dyndns.org and dnsalias.com
<i>dyns.net</i>	www.dyns.net
<i>tzo.com</i>	rh.tzo.com
<i>vavic.com</i>	Peanut Hull
<i>dipdns.net</i>	dipdnsserver.dipdns.com
<i>now.net.cn</i>	ip.todayisp.com
<i>dhs.org</i>	members.dhs.org
<i>easydns.com</i>	members.easydns.com
<i>genericDDNS</i>	Generic DDNS based on RFC2136.
<i>FortiGuardDDNS</i>	FortiGuard DDNS service.
<i>noip.com</i>	dynupdate.no-ip.com

ddns-server-ip	Generic DDNS server IP.	ipv4-address	Not Specified
ddns-sn	DDNS Serial Number.	string	Maximum length: 64
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 60 Maximum value: 86400
ddns-username	DDNS user name.	string	Maximum length: 64
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64
ddnsid	DDNS ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
monitor-interface <interface-name>	Monitored interface. Interface name.	string	Maximum length: 79
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35
update-interval	DDNS update interval (60 - 2592000 sec, default = 300).	integer	Minimum value: 60 Maximum value: 2592000
use-public-ip	Enable/disable use of public IP address.	option	-

Option	Description
<i>disable</i>	Disable use of public IP address.
<i>enable</i>	Enable use of public IP address.

config system dedicated-mgmt

Configure dedicated management.

```
config system dedicated-mgmt
    Description: Configure dedicated management.
    set default-gateway {ipv4-address}
    set dhcp-end-ip {ipv4-address}
    set dhcp-netmask {ipv4-netmask}
    set dhcp-server [enable|disable]
    set dhcp-start-ip {ipv4-address}
    set interface {string}
    set status [enable|disable]
end
```

config system dedicated-mgmt

Parameter	Description	Type	Size
default-gateway	Default gateway for dedicated management interface.	ipv4-address	Not Specified
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified
dhcp-server	Enable/disable DHCP server on management interface.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable DHCP server on management port.	
	<i>disable</i>	Disable DHCP server on management port.	
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified
interface	Dedicated management interface.	string	Maximum length: 15
status	Enable/disable dedicated management.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config system dhcp server

Configure DHCP servers.

```
config system dhcp server
    Description: Configure DHCP servers.
    edit <id>
        set auto-configuration [disable|enable]
        set conflicted-ip-timeout {integer}
        set ddns-auth [disable|tsig]
        set ddns-key {user}
        set ddns-keyname {string}
        set ddns-server-ip {ipv4-address}
        set ddns-ttl {integer}
        set ddns-update [disable|enable]
        set ddns-update-override [disable|enable]
        set ddns-zone {string}
        set default-gateway {ipv4-address}
        set dns-server1 {ipv4-address}
        set dns-server2 {ipv4-address}
        set dns-server3 {ipv4-address}
        set dns-server4 {ipv4-address}
        set dns-service [local|default|...]
        set domain {string}
    config exclude-range
        Description: Exclude one or more ranges of IP addresses from being assigned to
clients.
        edit <id>
            set end-ip {ipv4-address}
            set start-ip {ipv4-address}
        next
    end
    set filename {string}
```

```

set forticlient-on-net-status [disable|enable]
set interface {string}
set ip-mode [range|usrgrp]
config ip-range
    Description: DHCP IP range configuration.
    edit <id>
        set end-ip {ipv4-address}
        set start-ip {ipv4-address}
    next
end
set ipsec-lease-hold {integer}
set lease-time {integer}
set mac-acl-default-action [assign|block]
set netmask {ipv4-netmask}
set next-server {ipv4-address}
set ntp-server1 {ipv4-address}
set ntp-server2 {ipv4-address}
set ntp-server3 {ipv4-address}
set ntp-service [local|default|...]
config options
    Description: DHCP options.
    edit <id>
        set code {integer}
        set ip {user}
        set type [hex|string|...]
        set value {string}
    next
end
config reserved-address
    Description: Options for the DHCP server to assign IP settings to specific MAC
addresses.
    edit <id>
        set action [assign|block|...]
        set circuit-id {string}
        set circuit-id-type [hex|string]
        set description {var-string}
        set ip {ipv4-address}
        set mac {mac-address}
        set remote-id {string}
        set remote-id-type [hex|string]
        set type [mac|option82]
    next
end
set server-type [regular|ipsec]
set status [disable|enable]
set tftp-server <tftp-server1>, <tftp-server2>, ...
set timezone [01|02|...]
set timezone-option [disable|default|...]
set vci-match [disable|enable]
set vci-string <vci-string1>, <vci-string2>, ...
set wifi-ac-service [specify|local]
set wifi-acl {ipv4-address}
set wifi-ac2 {ipv4-address}
set wifi-ac3 {ipv4-address}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}

```

next
end

config system dhcp server

Parameter	Description	Type	Size
auto-configuration	Enable/disable auto configuration.	option	-
		Option	Description
		<i>disable</i>	Disable auto configuration.
		<i>enable</i>	Enable auto configuration.
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
ddns-auth	DDNS authentication mode.	option	-
		Option	Description
		<i>disable</i>	Disable DDNS authentication.
		<i>tsig</i>	TSIG based on RFC2845.
ddns-key	DDNS update key (base 64 encoding).	user	Not Specified
ddns-keyname	DDNS update key name.	string	Maximum length: 64
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400
ddns-update	Enable/disable DDNS update for DHCP.	option	-
		Option	Description
		<i>disable</i>	Disable DDNS update for DHCP.
		<i>enable</i>	Enable DDNS update for DHCP.
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-

Parameter	Description	Type	Size

	Option	Description	
	<i>disable</i>	Disable DDNS update override for DHCP.	
	<i>enable</i>	Enable DDNS update override for DHCP.	

ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified
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
dns-service	Options for assigning DNS servers to DHCP clients.	option	-

	Option	Description	
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.	
	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.	
	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.	

domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-

	Option	Description	
	<i>disable</i>	Disable FortiClient On-Net Status.	
	<i>enable</i>	Enable FortiClient On-Net Status.	

id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15

Parameter	Description	Type	Size
ip-mode	Method used to assign client IP.	option	-

Option	Description

<i>range</i>	Use range defined by start-ip/end-ip to assign client IP.
<i>usrgrp</i>	Use user-group defined method to assign client IP.

ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 0 Maximum value: 8640000
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

<i>assign</i>	Allow the DHCP server to assign IP settings to clients on the MAC access control list.
<i>block</i>	Block the DHCP server from assigning IP settings to clients on the MAC access control list.

netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified
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
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
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-

Option	Description

<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.
<i>default</i>	Clients are assigned the FortiGate's configured NTP servers.
<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.

Parameter	Description	Type	Size
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-
	Option	Description	
	<i>regular</i>	Regular DHCP service.	
	<i>ipsec</i>	DHCP over IPsec service.	
status	Enable/disable this DHCP configuration.	option	-
	Option	Description	
	<i>disable</i>	Do not use this DHCP server configuration.	
	<i>enable</i>	Use this DHCP server configuration.	
tftp-server <tftp-server>	One or more hostnames or IP addresses of the TFTP servers in quotes separated by spaces. TFTP server.	string	Maximum length: 63
timezone	Select the time zone to be assigned to DHCP clients.	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

Parameter	Description	Type	Size

Option	Description
14	(GMT-4:00) Atlantic Time (Canada)
77	(GMT-4:00) Georgetown
15	(GMT-4:00) La Paz
87	(GMT-4:00) Paraguay
16	(GMT-3:00) Santiago
17	(GMT-3:30) Newfoundland
18	(GMT-3:00) Brasilia
19	(GMT-3:00) Buenos Aires
20	(GMT-3:00) Nuuk (Greenland)
75	(GMT-3:00) Uruguay
21	(GMT-2:00) Mid-Atlantic
22	(GMT-1:00) Azores
23	(GMT-1:00) Cape Verde Is.
24	(GMT) Monrovia
80	(GMT) Greenwich Mean Time
79	(GMT) Casablanca
25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris
78	(GMT+1:00) Namibia
29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb
30	(GMT+1:00) West Central Africa
31	(GMT+2:00) Athens, Sofia, Vilnius
32	(GMT+2:00) Bucharest
33	(GMT+2:00) Cairo
34	(GMT+2:00) Harare, Pretoria
35	(GMT+2:00) Helsinki, Riga, Tallinn
36	(GMT+2:00) Jerusalem

Parameter	Description	Type	Size

Option	Description
37	(GMT+3:00) Baghdad
38	(GMT+3:00) Kuwait, Riyadh
83	(GMT+3:00) Moscow
84	(GMT+3:00) Minsk
40	(GMT+3:00) Nairobi
85	(GMT+3:00) Istanbul
41	(GMT+3:30) Tehran
42	(GMT+4:00) Abu Dhabi, Muscat
43	(GMT+4:00) Baku
39	(GMT+3:00) St. Petersburg, Volgograd
44	(GMT+4:30) Kabul
46	(GMT+5:00) Islamabad, Karachi, Tashkent
47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi
51	(GMT+5:30) Sri 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, Urumqi, 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

Parameter	Description	Type	Size

Option	Description
61	(GMT+9:00) Yakutsk
64	(GMT+10:00) Brisbane
65	(GMT+10:00) Canberra, Melbourne, Sydney
66	(GMT+10:00) Guam, Port Moresby
67	(GMT+10:00) Hobart
68	(GMT+10:00) Vladivostok
69	(GMT+10:00) Magadan
70	(GMT+11:00) Solomon Is., New Caledonia
71	(GMT+12:00) Auckland, Wellington
72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.
00	(GMT+12:00) Eniwetok, Kwajalein
82	(GMT+12:45) Chatham Islands
73	(GMT+13:00) Nuku'alofa
86	(GMT+13:00) Samoa
76	(GMT+14:00) Kiritimati

timezone-option	Options for the DHCP server to set the client's time zone.	option	-

Option	Description
<i>disable</i>	Do not set the client's time zone.
<i>default</i>	Clients are assigned the FortiGate's configured time zone.
<i>specify</i>	Specify the time zone to be assigned to DHCP clients.

vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-

Option	Description
<i>disable</i>	Disable VCI matching.
<i>enable</i>	Enable VCI matching.

vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255

Parameter	Description	Type	Size
wifi-ac-service	Options for assigning WiFi Access Controllers to DHCP clients	option	-
	Option	Description	
	<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.	
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.	
wifi-ac1	WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified
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
wins-server1	WINS server 1.	ipv4-address	Not Specified
wins-server2	WINS server 2.	ipv4-address	Not Specified

config exclude-range

Parameter	Description	Type	Size
end-ip	End of IP range.	ipv4-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IP range.	ipv4-address	Not Specified

config ip-range

Parameter	Description	Type	Size
end-ip	End of IP range.	ipv4-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IP range.	ipv4-address	Not Specified

config options

Parameter	Description	Type	Size
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	DHCP option IPs.	user	Not Specified
type	DHCP option type.	option	-
	Option	Description	
	<i>hex</i>	DHCP option in hex.	
	<i>string</i>	DHCP option in string.	
	<i>ip</i>	DHCP option in IP.	
	<i>fqdn</i>	DHCP option in domain search option format.	
value	DHCP option value.	string	Maximum length: 312

config reserved-address

Parameter	Description	Type	Size
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-
	Option	Description	
	<i>assign</i>	Configure the client with this MAC address like any other client.	
	<i>block</i>	Block the DHCP server from assigning IP settings to the client with this MAC address.	
	<i>reserved</i>	Assign the reserved IP address to the client with this MAC address.	
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312
circuit-id-type	DHCP option type.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>hex</i>	DHCP option in hex.	
	<i>string</i>	DHCP option in string.	
description	Description.	var-string	Maximum length: 255
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
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
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312
remote-id-type	DHCP option type.	option	-
	Option	Description	
	<i>hex</i>	DHCP option in hex.	
	<i>string</i>	DHCP option in string.	
type	DHCP reserved-address type.	option	-
	Option	Description	
	<i>mac</i>	Match with MAC address.	
	<i>option82</i>	Match with DHCP option 82.	

config system dhcp6 server

Configure DHCPv6 servers.

```
config system dhcp6 server
    Description: Configure DHCPv6 servers.
    edit <id>
        set dns-search-list [delegated|specify]
        set dns-server1 {ipv6-address}
        set dns-server2 {ipv6-address}
        set dns-server3 {ipv6-address}
        set dns-server4 {ipv6-address}
```



```

set dns-service [delegated|default|...]
set domain {string}
set interface {string}
set ip-mode [range|delegated]
config ip-range
    Description: DHCP IP range configuration.
    edit <id>
        set end-ip {ipv6-address}
        set start-ip {ipv6-address}
    next
end
set lease-time {integer}
set option1 {user}
set option2 {user}
set option3 {user}
config prefix-range
    Description: DHCP prefix configuration.
    edit <id>
        set end-prefix {ipv6-address}
        set prefix-length {integer}
        set start-prefix {ipv6-address}
    next
end
set rapid-commit [disable|enable]
set status [disable|enable]
set subnet {ipv6-prefix}
set upstream-interface {string}
next
end

```

config system dhcp6 server

Parameter	Description	Type	Size
dns-search-list	DNS search list options.	option	-
	Option	Description	
	<i>delegated</i>	Delegated the DNS search list.	
	<i>specify</i>	Specify the DNS search list.	
dns-server1	DNS server 1.	ipv6-address	Not Specified
dns-server2	DNS server 2.	ipv6-address	Not Specified
dns-server3	DNS server 3.	ipv6-address	Not Specified
dns-server4	DNS server 4.	ipv6-address	Not Specified
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>delegated</i>	Delegated DNS settings.	
	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.	
	<i>specify</i>	Specify up to 3 DNS servers in the DHCPv6 server configuration.	
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15
ip-mode	Method used to assign client IP.	option	-
	Option	Description	
	<i>range</i>	Use range defined by start IP/end IP to assign client IP.	
	<i>delegated</i>	Use delegated prefix method to assign client IP.	
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000
option1	Option 1.	user	Not Specified
option2	Option 2.	user	Not Specified
option3	Option 3.	user	Not Specified
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-
	Option	Description	
	<i>disable</i>	Do not allow rapid commit.	
	<i>enable</i>	Allow rapid commit.	
status	Enable/disable this DHCPv6 configuration.	option	-
	Option	Description	
	<i>disable</i>	Enable this DHCPv6 server configuration.	
	<i>enable</i>	Disable this DHCPv6 server configuration.	

Parameter	Description	Type	Size
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15

config ip-range

Parameter	Description	Type	Size
end-ip	End of IP range.	ipv6-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IP range.	ipv6-address	Not Specified

config prefix-range

Parameter	Description	Type	Size
end-prefix	End of prefix range.	ipv6-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128
start-prefix	Start of prefix range.	ipv6-address	Not Specified

config system dnp3-proxy



This command is available for model(s): FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure dnpproxy settings.

```
config system dnp3-proxy
    Description: Configure dnpproxy settings.
    set port {integer}
    set term-baudrate {integer}
    set term-databits {integer}
    set term-flowcontrol [none|xon_xoff|...]
    set term-parity [none|odd|...]
    set term-stopbits {integer}
end
```

config system dnp3-proxy

Parameter	Description	Type	Size
port	DNP3 TCPServer Port.	integer	Minimum value: 1 Maximum value: 65535

Parameter	Description	Type	Size
term-baudrate	Term Baudrate.	integer	Minimum value: 0 Maximum value: 4294967295
term-databits	Term Data Bits.	integer	Minimum value: 0 Maximum value: 65535
term-flowcontrol	Term Flow Control	option	-
	Option	Description	
	none	No flow control.	
	xon_xoff	Enable software flow control on both input and output.	
	hardware	Enable hardware flow control.	
term-parity	Term Parity	option	-
	Option	Description	
	none	No parity check.	
	odd	Odd parity check.	
	even	Even parity check.	
term-stopbits	Term Stop Bits.	integer	Minimum value: 0 Maximum value: 65535

config system dns

Configure DNS.

```
config system dns
    Description: Configure DNS.
    set cache-notfound-responses [disable|enable]
    set dns-cache-limit {integer}
    set dns-cache-ttl {integer}
    set dns-over-tls [disable|enable|...]
    set domain <domain1>, <domain2>, ...
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
```

```

set primary {ipv4-address}
set retry {integer}
set secondary {ipv4-address}
set server-hostname <hostname1>, <hostname2>, ...
set source-ip {ipv4-address}
set ssl-certificate {string}
set timeout {integer}
end

```

config system dns

Parameter	Description	Type	Size
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-
	Option	Description	
	<i>disable</i>	Disable cache NOTFOUND responses from DNS server.	
	<i>enable</i>	Enable cache NOTFOUND responses from DNS server.	
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400
dns-over-tls	Enable/disable/enforce DNS over TLS.	option	-
	Option	Description	
	<i>disable</i>	Disable DNS over TLS.	
	<i>enable</i>	Use TLS for DNS queries if TLS is available.	
	<i>enforce</i>	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.	
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127
interface	Specify outgoing interface to reach server.	string	Maximum length: 15

Parameter	Description	Type	Size								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.		
	Option	Description									
	auto	Set outgoing interface automatically.									
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.									
specify	Set outgoing interface manually.										
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified								
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified								
primary	Primary DNS server IP address.	ipv4-address	Not Specified								
retry	Number of times to retry (0 - 5).	integer	Minimum value: 0 Maximum value: 5								
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified								
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127								
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified								
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35								
timeout	DNS query timeout interval in seconds (1 - 10).	integer	Minimum value: 1 Maximum value: 10								

config system dns-database

Configure DNS databases.

```
config system dns-database
  Description: Configure DNS databases.
  edit <name>
    set allow-transfer {user}
    set authoritative [enable|disable]
    set contact {string}
  config dns-entry
    Description: DNS entry.
    edit <id>
      set canonical-name {string}
      set hostname {string}
```

```

        set ip {ipv4-address-any}
        set ipv6 {ipv6-address}
        set preference {integer}
        set status [enable|disable]
        set ttl {integer}
        set type [A|NS|...]
    next
end
set domain {string}
set forwarder {user}
set ip-master {ipv4-address-any}
set primary-name {string}
set source-ip {ipv4-address}
set status [enable|disable]
set ttl {integer}
set type [master|slave]
set view [shadow|public]
next
end

```

config system dns-database

Parameter	Description	Type	Size
allow-transfer	DNS zone transfer IP address list.	user	Not Specified
authoritative	Enable/disable authoritative zone.	option	-
	Option	Description	
	<i>enable</i>	Enable authoritative zone.	
	<i>disable</i>	Disable authoritative zone.	
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
domain	Domain name.	string	Maximum length: 255
forwarder	DNS zone forwarder IP address list.	user	Not Specified
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
name	Zone name.	string	Maximum length: 35
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified

Parameter	Description	Type	Size						
status	Enable/disable this DNS zone.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
ttl	Default time-to-live value for the entries of this DNS zone (0 - 2147483647 sec, default = 86400).	integer	Minimum value: 0 Maximum value: 2147483647						
type	Zone type (master to manage entries directly, slave to import entries from other zones).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>master</i></td><td>Master DNS zone, to manage entries directly.</td></tr><tr><td><i>slave</i></td><td>Slave DNS zone, to import entries from other DNS zones.</td></tr></table>	Option	Description	<i>master</i>	Master DNS zone, to manage entries directly.	<i>slave</i>	Slave DNS zone, to import entries from other DNS zones.		
Option	Description								
<i>master</i>	Master DNS zone, to manage entries directly.								
<i>slave</i>	Slave DNS zone, to import entries from other DNS zones.								
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shadow</i></td><td>Shadow DNS zone to serve internal clients.</td></tr><tr><td><i>public</i></td><td>Public DNS zone to serve public clients.</td></tr></table>	Option	Description	<i>shadow</i>	Shadow DNS zone to serve internal clients.	<i>public</i>	Public DNS zone to serve public clients.		
Option	Description								
<i>shadow</i>	Shadow DNS zone to serve internal clients.								
<i>public</i>	Public DNS zone to serve public clients.								

config dns-entry

Parameter	Description	Type	Size
canonical-name	Canonical name of the host.	string	Maximum length: 255
hostname	Name of the host.	string	Maximum length: 255
id	DNS entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IPv4 address of the host.	ipv4-address-any	Not Specified
ipv6	IPv6 address of the host.	ipv6-address	Not Specified

Parameter	Description	Type	Size
preference	DNS entry preference, 0 is the highest preference (0 - 65535, default = 10)	integer	Minimum value: 0 Maximum value: 65535
status	Enable/disable resource record status.	option	-
	Option	Description	
	<i>enable</i>	Enable resource record status.	
	<i>disable</i>	Disable resource record status.	
ttl	Time-to-live for this entry (0 to 2147483647 sec, default = 0).	integer	Minimum value: 0 Maximum value: 2147483647
type	Resource record type.	option	-
	Option	Description	
	<i>A</i>	Host type.	
	<i>NS</i>	Name server type.	
	<i>CNAME</i>	Canonical name type.	
	<i>MX</i>	Mail exchange type.	
	<i>AAAA</i>	IPv6 host type.	
	<i>PTR</i>	Pointer type.	
	<i>PTR_V6</i>	IPv6 pointer type.	

config system dns-server

Configure DNS servers.

```
config system dns-server
    Description: Configure DNS servers.
    edit <name>
        set dnsfilter-profile {string}
        set mode [recursive|non-recursive|...]
    next
end
```

config system dns-server

Parameter	Description	Type	Size
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35
mode	DNS server mode.	option	-
	Option	Description	
	<i>recursive</i>	Shadow DNS database and forward.	
	<i>non-recursive</i>	Public DNS database only.	
	<i>forward-only</i>	Forward only.	
name	DNS server name.	string	Maximum length: 15

config system dscp-based-priority

Configure DSCP based priority table.

```
config system dscp-based-priority
  Description: Configure DSCP based priority table.
  edit <id>
    set ds {integer}
    set priority [low|medium|...]
  next
end
```

config system dscp-based-priority

Parameter	Description	Type	Size
ds	DSCP(DiffServ) DS value (0 - 63).	integer	Minimum value: 0 Maximum value: 63
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295
priority	DSCP based priority level.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>low</i>	Low priority.	
	<i>medium</i>	Medium priority.	
	<i>high</i>	High priority.	

config system elbc



This command is available for model(s): FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure enhanced load balance cluster.

```
config system elbc
    Description: Configure enhanced load balance cluster.
    set graceful-upgrade [enable|disable]
    set hb-device <name1>, <name2>, ...
    set inter-chassis-support [enable|disable]
    set mode [none|forticontroller|...]
end
```

config system elbc

Parameter	Description	Type	Size
graceful-upgrade	enable/disable graceful upgrade	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
hb-device <name>	ELBC heartbeat device. set interface name	string	Maximum length: 79
inter-chassis-support	Enable/disable content-cluster across multiple chassis.	option	-
	Option	Description	
	<i>enable</i>	Enable content-cluster across multiple chassis.	
	<i>disable</i>	Disable content-cluster across multiple chassis.	
mode	ELBC mode.	option	-
	Option	Description	
	<i>none</i>	ELBC mode disabled.	
	<i>forticontroller</i>	FortiController.	
	<i>dual-forticontroller</i>	Dual-FortiController.	

config system email-server

Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features.

```
config system email-server
    Description: Configure the email server used by the FortiGate various things. For
    example, for sending email messages to users to support user authentication features.
    set authenticate [enable|disable]
    set password {password}
    set port {integer}
    set reply-to {string}
    set security [none|starttls|...]
    set server {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set ssl-min-proto-version [default|SSLv3|...]
```

```

set type {option}
set username {string}
set validate-server [enable|disable]
end

```

config system email-server

Parameter	Description	Type	Size
authenticate	Enable/disable authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable authentication.	
	<i>disable</i>	Disable authentication.	
password	SMTP server user password for authentication.	password	Not Specified
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535
reply-to	Reply-To email address.	string	Maximum length: 63
security	Connection security used by the email server.	option	-
	Option	Description	
	<i>none</i>	None.	
	<i>starttls</i>	STARTTLS.	
	<i>smtps</i>	SSL/TLS.	
server	SMTP server IP address or hostname.	string	Maximum length: 63
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	

Parameter	Description	Type	Size
	Option	Description	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
type	Use FortiGuard Message service or custom email server.	option	-
	Option	Description	
	<i>custom</i>	Use custom email server.	
username	SMTP server user name for authentication.	string	Maximum length: 63
validate-server	Enable/disable validation of server certificate.	option	-
	Option	Description	
	<i>enable</i>	Enable validation of server certificate.	
	<i>disable</i>	Disable validation of server certificate.	

config system external-resource

Configure external resource.

```

config system external-resource
    Description: Configure external resource.
    edit <name>
        set category {integer}
        set comments {var-string}
        set password {password}
        set refresh-rate {integer}
        set resource {string}
        set source-ip {ipv4-address}
        set status [enable|disable]
        set type [category|address|...]
        set username {string}
    next
end

```

config system external-resource

Parameter	Description	Type	Size
category	User resource category.	integer	Minimum value: 192 Maximum value: 221
comments	Comment.	var-string	Maximum length: 255
name	External resource name.	string	Maximum length: 35
password	HTTP basic authentication password.	password	Not Specified
refresh-rate	Time interval to refresh external resource (1 - 43200 min, default = 5 min).	integer	Minimum value: 1 Maximum value: 43200
resource	URI of external resource.	string	Maximum length: 511
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified
status	Enable/disable user resource.	option	-
	Option	Description	
	<i>enable</i>	Enable user resource.	
	<i>disable</i>	Disable user resource.	
type	User resource type.	option	-
	Option	Description	
	<i>category</i>	FortiGuard category.	
	<i>address</i>	Firewall IP address.	
	<i>domain</i>	Domain Name.	
	<i>malware</i>	Malware hash.	
username	HTTP basic authentication user name.	string	Maximum length: 64

config system fips-cc

Configure FIPS-CC mode.

```
config system fips-cc
    Description: Configure FIPS-CC mode.
    set entropy-token [enable|disable|...]
    set key-generation-self-test [enable|disable]
    set self-test-period {integer}
    set status [enable|disable]
end
```

config system fips-cc

Parameter	Description	Type	Size
entropy-token	Enable/disable/dynamic entropy token.	option	-
	Option	Description	
	<i>enable</i>	Enable entropy token to be present during boot process.	
	<i>disable</i>	Disable entropy token to be present during boot process.	
	<i>dynamic</i>	Dynamic detect entropy token to be present during boot process.	
key-generation-self-test	Enable/disable self tests after key generation.	option	-
	Option	Description	
	<i>enable</i>	Enable self tests after key generation.	
	<i>disable</i>	Disable self tests after key generation.	
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440
status	Enable/disable FIPS-CC mode.	option	-
	Option	Description	
	<i>enable</i>	Enable/disable FIPS-CC mode.	
	<i>disable</i>	Disable FIPS-CC mode.	

config system fm

Configure FM.

```

config system fm
    Description: Configure FM.
    set auto-backup [enable|disable]
    set id {string}
    set ip {ipv4-address}
    set ipsec [enable|disable]
    set scheduled-config-restore [enable|disable]
    set status [enable|disable]
    set vdom {string}
end

```

config system fm

Parameter	Description	Type	Size
auto-backup	Enable/disable automatic backup.	option	-
	Option	Description	
	<i>enable</i>	Enable automatic backup.	
	<i>disable</i>	Disable automatic backup.	
id	ID.	string	Maximum length: 35
ip	IP address.	ipv4-address	Not Specified
ipsec	Enable/disable IPsec.	option	-
	Option	Description	
	<i>enable</i>	Enable IPsec.	
	<i>disable</i>	Disable IPsec.	
scheduled-config-restore	Enable/disable scheduled configuration restore.	option	-
	Option	Description	
	<i>enable</i>	Enable scheduled configuration restore.	
	<i>disable</i>	Disable scheduled configuration restore.	
status	Enable/disable FM.	option	-
	Option	Description	
	<i>enable</i>	Enable FM.	
	<i>disable</i>	Disable FM.	
vdom	VDOM.	string	Maximum length: 31

config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
    Description: Configure FortiGuard services.
    set antispam-cache [enable|disable]
    set antispam-cache-mpercent {integer}
    set antispam-cache-ttl {integer}
    set antispam-expiration {integer}
    set antispam-force-off [enable|disable]
    set antispam-license {integer}
    set antispam-timeout {integer}
    set auto-join-forticloud [enable|disable]
    set ddns-server-ip {ipv4-address}
    set ddns-server-port {integer}
    set fortiguard-anycast [enable|disable]
    set fortiguard-anycast-source [fortinet|aws|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set load-balance-servers {integer}
    set outbreak-prevention-cache [enable|disable]
    set outbreak-prevention-cache-mpercent {integer}
    set outbreak-prevention-cache-ttl {integer}
    set outbreak-prevention-expiration {integer}
    set outbreak-prevention-force-off [enable|disable]
    set outbreak-prevention-license {integer}
    set outbreak-prevention-timeout {integer}
    set port [8888|53|...]
    set protocol [udp|http|...]
    set proxy-password {password}
    set proxy-server-ip {ipv4-address}
    set proxy-server-port {integer}
    set proxy-username {string}
    set sandbox-region {string}
    set sdns-server-ip {user}
    set sdns-server-port {integer}
    set service-account-id {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set update-server-location [usa|any]
    set webfilter-cache [enable|disable]
    set webfilter-cache-ttl {integer}
    set webfilter-expiration {integer}
    set webfilter-force-off [enable|disable]
    set webfilter-license {integer}
    set webfilter-timeout {integer}
end
```

config system fortiguard

Parameter	Description	Type	Size
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-
	Option	Description	
	<i>enable</i>	Enable FortiGuard antispam request caching.	
	<i>disable</i>	Disable FortiGuard antispam request caching.	
antispam-cache-mppercent	Maximum percent of FortiGate memory the antispam cache is allowed to use (1 - 15%).	integer	Minimum value: 1 Maximum value: 15
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds (300 - 86400). Lower times reduce the cache size. Higher times may improve performance since the cache will have more entries.	integer	Minimum value: 300 Maximum value: 86400
antispam-expiration	Expiration date of the FortiGuard antispam contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-
	Option	Description	
	<i>enable</i>	Turn off the FortiGuard antispam service.	
	<i>disable</i>	Allow the FortiGuard antispam service.	
antispam-license	Interval of time between license checks for the FortiGuard antispam contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
antispam-timeout	Antispam query time out (1 - 30 sec, default = 7).	integer	Minimum value: 1 Maximum value: 30
auto-join-forticloud *	Automatically connect to and login to FortiCloud.	option	-

Parameter	Description	Type	Size
	Option	Description	
	enable	Enable automatic connection and login to FortiCloud.	
	disable	Disable automatic connection and login to FortiCloud.	
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
fortiguard-anycast	Enable/disable use of FortiGuard's anycast network.	option	-
	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.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
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
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-

Option	Description
<i>enable</i>	Enable FortiGuard antivirus caching.
<i>disable</i>	Disable FortiGuard antivirus caching.

outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use (1 - 15%, default = 2).	integer	Minimum value: 1 Maximum value: 15
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries (300 - 86400 sec, default = 300).	integer	Minimum value: 300 Maximum value: 86400
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-

Option	Description
<i>enable</i>	Turn off FortiGuard antivirus service.
<i>disable</i>	Allow the FortiGuard antivirus service.

outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out (1 - 30 sec, default = 7).	integer	Minimum value: 1 Maximum value: 30

Parameter	Description	Type	Size										
port	Port used to communicate with the FortiGuard servers.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8888</td><td>port 8888 for server communication.</td></tr><tr><td>53</td><td>port 53 for server communication.</td></tr><tr><td>80</td><td>port 80 for server communication.</td></tr><tr><td>443</td><td>port 443 for server communication.</td></tr></table>	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.		
	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.											
protocol	Protocol used to communicate with the FortiGuard servers.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>UDP for server communication (for use by FortiGuard or FortiManager).</td></tr><tr><td>http</td><td>HTTP for server communication (for use only by FortiManager).</td></tr><tr><td>https</td><td>HTTPS for server communication (for use by FortiGuard or FortiManager).</td></tr></table>	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).				
	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).												
proxy-password	Proxy user password.	password	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										
sandbox-region	Cloud sandbox region.	string	Maximum length: 63										
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										
service-account-id *	Service account ID.	string	Maximum length: 50										
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified										

Parameter	Description	Type	Size						
source-ipv6	Source IPv6 address used to communicate with FortiGuard.	ipv6-address	Not Specified						
update-server-location	Signature update server location.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>usa</td><td>FGD servers in United States.</td></tr><tr><td>any</td><td>FGD servers in any location.</td></tr></table>	Option	Description	usa	FGD servers in United States.	any	FGD servers in any location.		
Option	Description								
usa	FGD servers in United States.								
any	FGD servers in any location.								
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiGuard web filter caching.</td></tr><tr><td>disable</td><td>Disable FortiGuard web filter caching.</td></tr></table>	Option	Description	enable	Enable FortiGuard web filter caching.	disable	Disable FortiGuard web filter caching.		
Option	Description								
enable	Enable FortiGuard web filter caching.								
disable	Disable FortiGuard web filter caching.								
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds (300 - 86400).	integer	Minimum value: 300 Maximum value: 86400						
webfilter-expiration	Expiration date of the FortiGuard web filter contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295						
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Turn off the FortiGuard web filtering service.</td></tr><tr><td>disable</td><td>Allow the FortiGuard web filtering service to operate.</td></tr></table>	Option	Description	enable	Turn off the FortiGuard web filtering service.	disable	Allow the FortiGuard web filtering service to operate.		
Option	Description								
enable	Turn off the FortiGuard web filtering service.								
disable	Allow the FortiGuard web filtering service to operate.								
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295						
webfilter-timeout	Web filter query time out (1 - 30 sec, default = 7).	integer	Minimum value: 1 Maximum value: 30						

* This parameter may not exist in some models.

config system fortimanager

Configure FortiManager.

```
config system fortimanager
  Description: Configure FortiManager.
  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]
  set ip {ipv4-address-any}
  set ipsec [enable|disable]
  set vdom {string}
end
```

config system fortimanager

Parameter	Description	Type	Size
central-management	Enable/disable FortiManager central management.	option	-
		Option	Description
		<i>enable</i>	Enable central management.
		<i>disable</i>	Disable central management.
central-mgmt-auto-backup	Enable/disable central management auto backup.	option	-
		Option	Description
		<i>enable</i>	Enable auto backup.
		<i>disable</i>	Disable auto backup.
central-mgmt-schedule-config-restore	Enable/disable central management schedule config restore.	option	-
		Option	Description
		<i>enable</i>	Enable central management scheduled restore.
		<i>disable</i>	Disable central management scheduled restore.
central-mgmt-schedule-script-restore	Enable/disable central management schedule script restore.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable central management scheduled restore.	
	<i>disable</i>	Disable central management scheduled restore.	
ip	IP address.	ipv4-address-any	Not Specified
ipsec	Enable/disable FortiManager IPsec tunnel.	option	-
	Option	Description	
	<i>enable</i>	Enable FortiManager IPsec tunnel.	
	<i>disable</i>	Disable FortiManager IPsec tunnel.	
vdom	Virtual domain name.	string	Maximum length: 31

config system fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
  Description: Configure FortiSandbox.
  set email {string}
  set enc-algorithm [default|high|...]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
end
```

config system fortisandbox

Parameter	Description	Type	Size
email	Notifier email address.	string	Maximum length: 63
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-
	Option	Description	
	<i>default</i>	SSL communication with high and medium encryption algorithms.	
	<i>high</i>	SSL communication with high encryption algorithms.	

Parameter	Description	Type	Size
	Option	Description	
	<i>low</i>	SSL communication with low encryption algorithms.	
server	Server address of the remote FortiSandbox.	string	Maximum length: 63
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-
	Option	Description	
	<i>default</i>	Follow system global setting.	
	<i>SSLv3</i>	SSLv3.	
	<i>TLSv1</i>	TLSv1.	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
status	Enable/disable FortiSandbox.	option	-
	Option	Description	
	<i>enable</i>	Enable FortiSandbox.	
	<i>disable</i>	Disable FortiSandbox.	

config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fsso-polling
    Description: Configure Fortinet Single Sign On (FSSO) server.
    set auth-password {password}
    set authentication [enable|disable]
    set listening-port {integer}
    set status [enable|disable]
end
```

config system fsso-polling

Parameter	Description	Type	Size
auth-password	Password to connect to FSSO Agent.	password	Not Specified

Parameter	Description	Type	Size
authentication	Enable/disable FSSO Agent Authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable FSSO Agent Authentication.	
	<i>disable</i>	Disable FSSO Agent Authentication.	
listening-port	Listening port to accept clients (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable FSSO Polling Mode.	option	-
	Option	Description	
	<i>enable</i>	Enable FSSO Polling Mode.	
	<i>disable</i>	Disable FSSO Polling Mode.	

config system ftm-push

Configure FortiToken Mobile push services.

```
config system ftm-push
    Description: Configure FortiToken Mobile push services.
    set server-ip {ipv4-address}
    set server-port {integer}
    set status [enable|disable]
end
```

config system ftm-push

Parameter	Description	Type	Size
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
server-port	Port to communicate with FortiToken Mobile push services server (1 - 65535, default = 4433).	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable the use of FortiToken Mobile push services.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable FortiToken Mobile push services.	
	<i>disable</i>	Disable FortiToken Mobile push services.	

config system geneve

Configure GENEVE devices.

```
config system geneve
  Description: Configure GENEVE devices.
  edit <name>
    set dstport {integer}
    set interface {string}
    set ip-version [ipv4-unicast|ipv6-unicast]
    set remote-ip {ipv4-address}
    set remote-ip6 {ipv6-address}
    set vni {integer}
  next
end
```

config system geneve

Parameter	Description	Type	Size
dstport	GENEVE destination port (1 - 65535, default = 6081).	integer	Minimum value: 1 Maximum value: 65535
interface	Outgoing interface for GENEVE encapsulated traffic.	string	Maximum length: 15
ip-version	IP version to use for the GENEVE interface and so for communication over the GENEVE. IPv4 or IPv6 unicast.	option	-
	Option	Description	
	<i>ipv4-unicast</i>	Use IPv4 unicast addressing over the GENEVE.	
	<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the GENEVE.	
name	GENEVE device or interface name. Must be an unique interface name.	string	Maximum length: 15
remote-ip	IPv4 address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv4-address	Not Specified

Parameter	Description	Type	Size
remote-ip6	IPv6 IP address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv6-address	Not Specified
vni	GENEVE network ID.	integer	Minimum value: 0 Maximum value: 16777215

config system geoip-override

Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.

```
config system geoip-override
    Description: Configure geographical location mapping for IP address(es) to override
mappings from FortiGuard.
    edit <name>
        set country-id {string}
        set description {string}
        config ip-range
            Description: Table of IP ranges assigned to country.
            edit <id>
                set end-ip {ipv4-address}
                set start-ip {ipv4-address}
            next
        next
    end
end
```

config system geoip-override

Parameter	Description	Type	Size
country-id	Two character Country ID code.	string	Maximum length: 2
description	Description.	string	Maximum length: 127
name	Location name.	string	Maximum length: 63

config ip-range

Parameter	Description	Type	Size
end-ip	Final IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
id	ID number for individual entry in the IP-Range table.	integer	Minimum value: 0 Maximum value: 65535
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified

config system global

Configure global attributes.

```
config system global
  Description: Configure global attributes.
  set admin-concurrent [enable|disable]
  set admin-console-timeout {integer}
  set admin-hsts-max-age {integer}
  set admin-https-pki-required [enable|disable]
  set admin-https-redirect [enable|disable]
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admin-lockout-duration {integer}
  set admin-lockout-threshold {integer}
  set admin-login-max {integer}
  set admin-maintainer [enable|disable]
  set admin-port {integer}
  set admin-reset-button [enable|disable]
  set admin-restrict-local [enable|disable]
  set admin-scp [enable|disable]
  set admin-server-cert {string}
  set admin-sport {integer}
  set admin-ssh-grace-time {integer}
  set admin-ssh-password [enable|disable]
  set admin-ssh-port {integer}
  set admin-ssh-v1 [enable|disable]
  set admin-telnet [enable|disable]
  set admin-telnet-port {integer}
  set admintimeout {integer}
  set alias {string}
  set allow-traffic-redirect [enable|disable]
  set anti-replay [disable|loose|...]
  set arp-max-entry {integer}
  set auth-cert {string}
  set auth-http-port {integer}
  set auth-https-port {integer}
  set auth-keepalive [enable|disable]
  set auth-session-limit [block-new|logout-inactive]
```

```
set auto-auth-extension-device [enable|disable]
set autorun-log-fsck [enable|disable]
set av-affinity {string}
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set batch-cmdb [enable|disable]
set block-session-timer {integer}
set br-fdb-max-entry {integer}
set cert-chain-max {integer}
set cfg-revert-timeout {integer}
set cfg-save [automatic|manual|...]
set check-protocol-header [loose|strict]
set check-reset-range [strict|disable]
set cli-audit-log [enable|disable]
set cloud-communication [enable|disable]
set clt-cert-req [enable|disable]
set cpu-use-threshold {integer}
set csr-ca-attribute [enable|disable]
set daily-restart [enable|disable]
set default-service-source-port {user}
set device-identification-active-scan-delay {integer}
set device-idle-timeout {integer}
set dh-params [1024|1536|...]
set dnsproxy-worker-count {integer}
set dst [enable|disable]
set failtime {integer}
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set fec-port {integer}
set fgd-alert-subscription {option1}, {option2}, ...
set forticontroller-proxy [enable|disable]
set forticontroller-proxy-port {integer}
set fortiextender [disable|enable]
set fortiextender-data-port {integer}
set fortiextender-vlan-mode [enable|disable]
set fortiservice-port {integer}
set fortitoken-cloud [enable|disable]
set gui-allow-default-hostname [enable|disable]
set gui-allow-incompatible-fabric-fgt [enable|disable]
set gui-certificates [enable|disable]
set gui-custom-language [enable|disable]
set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
set gui-date-time-source [system|browser]
set gui-device-latitude {string}
set gui-device-longitude {string}
set gui-display-hostname [enable|disable]
set gui-fortisandbox-cloud [enable|disable]
set gui-ipv6 [enable|disable]
set gui-lines-per-page {integer}
set gui-theme [green|neutrino|...]
set gui-wireless-opensecurity [enable|disable]
set honor-df [enable|disable]
set hostname {string}
set hw-switch-ether-filter [enable|disable]
set igmp-state-limit {integer}
set internal-switch-speed {option1}, {option2}, ...
```

```
set interval {integer}
set ip-src-port-range {user}
set ips-affinity {string}
set ipsec-asic-offload [enable|disable]
set ipsec-hmac-offload [enable|disable]
set ipsec-soft-dec-async [enable|disable]
set ipv6-accept-dad {integer}
set ipv6-allow-anycast-probe [enable|disable]
set language [english|french|...]
set ldapconntimeout {integer}
set legacy-poe-device-support [enable|disable]
set lldp-reception [enable|disable]
set lldp-transmission [enable|disable]
set log-ssl-connection [enable|disable]
set log-uuid-address [enable|disable]
set log-uuid-policy [enable|disable]
set login-timestamp [enable|disable]
set long-vdom-name [enable|disable]
set management-vdom {string}
set max-dlpstat-memory {integer}
set max-route-cache-size {integer}
set memory-use-threshold-extreme {integer}
set memory-use-threshold-green {integer}
set memory-use-threshold-red {integer}
set miglog-affinity {string}
set miglogd-children {integer}
set multi-factor-authentication [optional|mandatory]
set ndp-max-entry {integer}
set per-user-bwl [enable|disable]
set pmtu-discovery [enable|disable]
set policy-auth-concurrent {integer}
set post-login-banner [disable|enable]
set pre-login-banner [enable|disable]
set private-data-encryption [disable|enable]
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
set proxy-auth-timeout {integer}
set proxy-cipher-hardware-acceleration [disable|enable]
set proxy-kxp-hardware-acceleration [disable|enable]
set proxy-re-authentication-mode [session|traffic|...]
set proxy-worker-count {integer}
set radius-port {integer}
set reboot-upon-config-restore [enable|disable]
set refresh {integer}
set remoteauthtimeout {integer}
set reset-sessionless-tcp [enable|disable]
set restart-time {user}
set revision-backup-on-logout [enable|disable]
set revision-image-auto-backup [enable|disable]
set scanunit-count {integer}
set security-rating-result-submission [enable|disable]
set security-rating-run-on-schedule [enable|disable]
set send-pmtu-icmp [enable|disable]
set show-backplane-intf [enable|disable]
set snat-route-change [enable|disable]
set special-file-23-support [disable|enable]
```

```
set split-port {user}
set ssd-trim-date {integer}
set ssd-trim-freq [never|hourly|...]
set ssd-trim-hour {integer}
set ssd-trim-min {integer}
set ssd-trim-weekday [sunday|monday|...]
set ssh-cbc-cipher [enable|disable]
set ssh-hmac-md5 [enable|disable]
set ssh-kex-shal [enable|disable]
set ssh-mac-weak [enable|disable]
set ssl-min-proto-version [SSLv3|TLSv1|...]
set ssl-static-key-ciphers [enable|disable]
set sslvpn-cipher-hardware-acceleration [enable|disable]
set sslvpn-kxp-hardware-acceleration [enable|disable]
set sslvpn-max-worker-count {integer}
set sslvpn-plugin-version-check [enable|disable]
set strict-dirty-session-check [enable|disable]
set strong-crypto [enable|disable]
set switch-controller [disable|enable]
set switch-controller-reserved-network {ipv4-classnet}
set sys-perf-log-interval {integer}
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-option [enable|disable]
set tcp-timewait-timer {integer}
set tftp [enable|disable]
set timezone [01|02|...]
set traffic-priority [tos|dscp]
set traffic-priority-level [low|medium|...]
set two-factor-email-expiry {integer}
set two-factor-fac-expiry {integer}
set two-factor-ftk-expiry {integer}
set two-factor-ftm-expiry {integer}
set two-factor-sms-expiry {integer}
set udp-idle-timer {integer}
set url-filter-affinity {string}
set url-filter-count {integer}
set user-server-cert {string}
set vdom-mode [no-vdom|split-vdom|...]
set vip-arp-range [unlimited|restricted]
set virtual-switch-vlan [enable|disable]
set wad-affinity {string}
set wad-csvc-cs-count {integer}
set wad-csvc-db-count {integer}
set wad-memory-change-granularity {integer}
set wad-source-affinity [disable|enable]
set wad-worker-count {integer}
set wifi-ca-certificate {string}
set wifi-certificate {string}
set wimax-4g-usb [enable|disable]
set wireless-controller [enable|disable]
set wireless-controller-port {integer}
set wireless-mode [ac|client|...]
```

end

config system global

Parameter	Description	Type	Size						
admin-concurrent	Enable/disable concurrent administrator logins. (Use policy-auth-concurrent for firewall authenticated users.)	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable admin concurrent login.</td></tr><tr><td><i>disable</i></td><td>Disable admin concurrent login.</td></tr></table>	Option	Description	<i>enable</i>	Enable admin concurrent login.	<i>disable</i>	Disable admin concurrent login.		
Option	Description								
<i>enable</i>	Enable admin concurrent login.								
<i>disable</i>	Disable admin concurrent login.								
admin-console-timeout	Console login timeout that overrides the admintimeout value. (15 - 300 seconds) (15 seconds to 5 minutes). 0 the default, disables this timeout.	integer	Minimum value: 15 Maximum value: 300						
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-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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.</td></tr><tr><td><i>disable</i></td><td>Admin users can login by providing a valid certificate or password.</td></tr></table>	Option	Description	<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.	<i>disable</i>	Admin users can login by providing a valid certificate or password.		
Option	Description								
<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.								
<i>disable</i>	Admin users can login by providing a valid certificate or password.								
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirecting HTTP administration access to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirecting HTTP administration access to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.	<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.		
Option	Description								
<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.								
<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.								
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tlsv1-1</i></td><td>TLS 1.1.</td></tr></table>	Option	Description	<i>tlsv1-1</i>	TLS 1.1.				
Option	Description								
<i>tlsv1-1</i>	TLS 1.1.								

Parameter	Description	Type	Size

Option	Description
<i>tlsv1-2</i>	TLS 1.2.
<i>tlsv1-3</i>	TLS 1.3.

admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 1 Maximum value: 2147483647
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-login-max	Maximum number of administrators who can be logged in at the same time (1 - 100, default = 100)	integer	Minimum value: 1 Maximum value: 100
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
<i>enable</i>	Enable login for special user (maintainer).
<i>disable</i>	Disable login for special user (maintainer).

admin-port	Administrative access port for HTTP. (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535
admin-reset-button *	press the reset button can reset to factory default	option	-

Option	Description
<i>enable</i>	press the reset button can reset to factory default
<i>disable</i>	press the reset button cannot reset to factory default

Parameter	Description	Type	Size						
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running. (default = disable)	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local admin authentication restriction.</td></tr><tr><td><i>disable</i></td><td>Disable local admin authentication restriction.</td></tr></table>	Option	Description	<i>enable</i>	Enable local admin authentication restriction.	<i>disable</i>	Disable local admin authentication restriction.		
Option	Description								
<i>enable</i>	Enable local admin authentication restriction.								
<i>disable</i>	Disable local admin authentication restriction.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow system configuration download by SCP.</td></tr><tr><td><i>disable</i></td><td>Disable allow system configuration download by SCP.</td></tr></table>	Option	Description	<i>enable</i>	Enable allow system configuration download by SCP.	<i>disable</i>	Disable allow system configuration download by SCP.		
Option	Description								
<i>enable</i>	Enable allow system configuration download by SCP.								
<i>disable</i>	Disable allow system configuration download by SCP.								
admin-server-cert	Server certificate that the FortiGate uses for HTTPS administrative connections.	string	Maximum length: 35						
admin-sport	Administrative access port for HTTPS. (1 - 65535, default = 443).	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 (10 - 3600 sec (1 hour), default 120).	integer	Minimum value: 10 Maximum value: 3600						
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password authentication for SSH admin access.</td></tr><tr><td><i>disable</i></td><td>Disable password authentication for SSH admin access.</td></tr></table>	Option	Description	<i>enable</i>	Enable password authentication for SSH admin access.	<i>disable</i>	Disable password authentication for SSH admin access.		
Option	Description								
<i>enable</i>	Enable password authentication for SSH admin access.								
<i>disable</i>	Disable password authentication for SSH admin access.								
admin-ssh-port	Administrative access port for SSH. (1 - 65535, default = 22).	integer	Minimum value: 1 Maximum value: 65535						
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable SSH v1 compatibility.	
	<i>disable</i>	Disable SSH v1 compatibility.	
admin-telnet	Enable/disable TELNET service.	option	-
	Option	Description	
	<i>enable</i>	Enable TELNET service.	
	<i>disable</i>	Disable TELNET service.	
admin-telnet-port	Administrative access port for TELNET. (1 - 65535, default = 23).	integer	Minimum value: 1 Maximum value: 65535
admintimeout	Number of minutes before an idle administrator session times out (5 - 480 minutes (8 hours), default = 5). A shorter idle timeout is more secure.	integer	Minimum value: 1 Maximum value: 480
alias	Alias for your FortiGate unit.	string	Maximum length: 35
allow-traffic-redirect	Disable to allow traffic to be routed back on a different interface.	option	-
	Option	Description	
	<i>enable</i>	Enable allow traffic redirect.	
	<i>disable</i>	Disable allow traffic redirect.	
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-
	Option	Description	
	<i>disable</i>	Disable anti-replay check.	
	<i>loose</i>	Loose anti-replay check.	
	<i>strict</i>	Strict anti-replay check.	
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table (131072 - 2147483647, default = 131072).	integer	Minimum value: 131072 Maximum value: 2147483647

Parameter	Description	Type	Size
auth-cert	Server certificate that the FortiGate uses for HTTPS firewall authentication connections.	string	Maximum length: 35
auth-http-port	User authentication HTTP port. (1 - 65535, default = 80).	integer	Minimum value: 1 Maximum value: 65535
auth-https-port	User authentication HTTPS port. (1 - 65535, default = 443).	integer	Minimum value: 1 Maximum value: 65535
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-

Option	Description
<i>enable</i>	Enable use of keep alive to extend authentication.
<i>disable</i>	Disable use of keep alive to extend authentication.

auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-

Option	Description
<i>block-new</i>	Block new user authentication attempts.
<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.

auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-

Option	Description
<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.

autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-

Option	Description
<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.
<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.

Parameter	Description	Type	Size
av-affinity *	Affinity setting for AV scanning (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79
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
<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.
<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.
<i>one-shot</i>	Bypass the antivirus system when memory is low.

av-failopen-session	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen.	option	-

Option	Description
<i>enable</i>	Enable AV fail open session option.
<i>disable</i>	Disable AV fail open session option.

batch-cmdb	Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.	option	-

Option	Description
<i>enable</i>	Enable batch mode to execute in CMDB server.
<i>disable</i>	Disable batch mode to execute in CMDB server.

block-session-timer	Duration in seconds for blocked sessions (1 - 300 sec (5 minutes), default = 30).	integer	Minimum value: 1 Maximum value: 300

br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647

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
cfg-revert-timeout	Time-out for reverting to the last saved configuration.	integer	Minimum value: 10 Maximum value: 4294967295
cfg-save	Configuration file save mode for CLI changes.	option	-

Option	Description
<i>automatic</i>	Automatically save config.
<i>manual</i>	Manually save config.
<i>revert</i>	Manually save config and revert the config when timeout.

check-protocol-header	Level of checking performed on protocol headers. Strict checking is more thorough but may affect performance. Loose checking is ok in most cases.	option	-

Option	Description
<i>loose</i>	Check protocol header loosely.
<i>strict</i>	Check protocol header strictly.

check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-

Option	Description
<i>strict</i>	Check RST range strictly.
<i>disable</i>	Disable RST range check.

cli-audit-log	Enable/disable CLI audit log.	option	-

Option	Description
<i>enable</i>	Enable CLI audit log.
<i>disable</i>	Disable CLI audit log.

Parameter	Description	Type	Size
cloud-communication	Enable/disable all cloud communication.	option	-
	Option	Description	
	<i>enable</i>	Allow cloud communication.	
	<i>disable</i>	Disable all cloud-related settings.	
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-
	Option	Description	
	<i>enable</i>	Enable require client certificate for GUI login.	
	<i>disable</i>	Disable require client certificate for GUI login.	
cpu-use-threshold	Threshold at which CPU usage is reported. (% of total CPU, default = 90).	integer	Minimum value: 50 Maximum value: 99
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-
	Option	Description	
	<i>enable</i>	Enable CA attribute in CSR.	
	<i>disable</i>	Disable CA attribute in CSR.	
daily-restart	Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.	option	-
	Option	Description	
	<i>enable</i>	Enable daily reboot of the FortiGate.	
	<i>disable</i>	Disable daily reboot of the FortiGate.	
default-service-source-port	Default service source port range. (default=1-65535)	user	Not Specified
device-identification-active-scan-delay	Number of seconds to passively scan a device before performing an active scan. (20 - 3600 sec, (20 sec to 1 hour), default = 90).	integer	Minimum value: 20 Maximum value: 3600

Parameter	Description	Type	Size
device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out. (30 - 31536000 sec (30 sec to 1 year), default = 300).	integer	Minimum value: 30 Maximum value: 31536000
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.

dnsproxy-worker-count	DNS proxy worker count. For a FortiGate unit with multiple logical CPUs, the number of DNS processes may be set to 1 to the number of logical CPUs.	integer	Minimum value: 1 Maximum value: 8 **
dst	Enable/disable daylight saving time.	option	-

Option	Description
<i>enable</i>	Enable daylight saving time.
<i>disable</i>	Disable daylight saving time.

failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295
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	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable FortiGuard statistics.	
	<i>disable</i>	Disable FortiGuard statistics.	
fds-statistics-period	FortiGuard statistics collection period in minutes. (1 - 1440 min (1 min to 24 hours), default = 60).	integer	Minimum value: 1 Maximum value: 1440
fec-port	Local UDP port for Forward Error Correction (49152 - 65535).	integer	Minimum value: 49152 Maximum value: 65535
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-
	Option	Description	
	<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.	
	<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.	
	<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.	
	<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.	
	<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.	
	<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.	
forticontroller-proxy *	Enable/disable FortiController proxy.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
forticontroller-proxy-port *	FortiController proxy port (1024 - 49150).	integer	Minimum value: 1024 Maximum value: 49150
fortiextender	Enable/disable FortiExtender.	option	-
	Option	Description	
	<i>disable</i>	Disable FortiExtender controller.	
	<i>enable</i>	Enable FortiExtender controller.	

Parameter	Description	Type	Size						
fortiextender-data-port	FortiExtender data port (1024 - 49150, default = 25246).	integer	Minimum value: 1024 Maximum value: 49150						
fortiextender-vlan-mode	Enable/disable FortiExtender VLAN mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiExtender VLAN mode.</td></tr><tr><td><i>disable</i></td><td>Disable FortiExtender VLAN mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiExtender VLAN mode.	<i>disable</i>	Disable FortiExtender VLAN mode.		
Option	Description								
<i>enable</i>	Enable FortiExtender VLAN mode.								
<i>disable</i>	Disable FortiExtender VLAN mode.								
fortiservice-port	FortiService port (1 - 65535, default = 8013). Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535						
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiToken Cloud service.</td></tr><tr><td><i>disable</i></td><td>Disable FortiToken Cloud service.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiToken Cloud service.	<i>disable</i>	Disable FortiToken Cloud service.		
Option	Description								
<i>enable</i>	Enable FortiToken Cloud service.								
<i>disable</i>	Disable FortiToken Cloud service.								
gui-allow-default-hostname	Enable/disable the GUI warning about using a default hostname	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Stop the warning in the GUI.</td></tr><tr><td><i>disable</i></td><td>Show the warning in the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Stop the warning in the GUI.	<i>disable</i>	Show the warning in the GUI.		
Option	Description								
<i>enable</i>	Stop the warning in the GUI.								
<i>disable</i>	Show the warning in the GUI.								
gui-allow-incompatible-fabric-ftg *	Enable/disable Allow FGT with incompatible firmware to be treated as compatible in security fabric on the GUI. May cause unexpected error.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.		
Option	Description								
<i>enable</i>	Display the feature in GUI.								
<i>disable</i>	Do not display the feature in GUI.								
gui-certificates	Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Display the feature in GUI.	
	<i>disable</i>	Do not display the feature in GUI.	
gui-custom-language	Enable/disable custom languages in GUI.	option	-
	Option	Description	
	<i>enable</i>	Display the feature in GUI.	
	<i>disable</i>	Do not display the feature in GUI.	
gui-date-format	Default date format used throughout GUI.	option	-
	Option	Description	
	<i>yyyy/MM/dd</i>	Year/Month/Day.	
	<i>dd/MM/yyyy</i>	Day/Month/Year.	
	<i>MM/dd/yyyy</i>	Month/Day/Year.	
	<i>yyyy-MM-dd</i>	Year-Month-Day.	
	<i>dd-MM-yyyy</i>	Day-Month-Year.	
	<i>MM-dd-yyyy</i>	Month-Day-Year.	
gui-date-time-source	Source from which the FortiGate GUI uses to display date and time entries.	option	-
	Option	Description	
	<i>system</i>	Use this FortiGate unit's configured timezone.	
	<i>browser</i>	Use the web browser's timezone.	
gui-device-latitude	Add the latitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19
gui-device-longitude	Add the longitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19
gui-display-hostname	Enable/disable displaying the FortiGate's hostname on the GUI login page.	option	-
	Option	Description	
	<i>enable</i>	Display the feature in GUI.	
	<i>disable</i>	Do not display the feature in GUI.	

Parameter	Description	Type	Size
gui-fortisandbox-cloud	Enable/disable displaying FortiSandbox Cloud on the GUI.	option	-

Option	Description
<i>enable</i>	Display the feature in GUI.
<i>disable</i>	Do not display the feature in GUI.

gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-

Option	Description
<i>enable</i>	Display the feature in GUI.
<i>disable</i>	Do not display the feature in GUI.

gui-lines-per-page	Number of lines to display per page for web administration.	integer	Minimum value: 20 Maximum value: 1000

gui-theme	Color scheme for the administration GUI.	option	-

Option	Description
<i>green</i>	Green theme.
<i>neutrino</i>	Neutrino theme.
<i>blue</i>	Light blue theme.
<i>melongene</i>	Melongene theme (eggplant color).
<i>mariner</i>	Mariner theme (dark blue color).

gui-wireless-opensecurity	Enable/disable wireless open security option on the GUI.	option	-

Option	Description
<i>enable</i>	Display the feature in GUI.
<i>disable</i>	Do not display the feature in GUI.

honor-df	Enable/disable honoring of Don't-Fragment (DF) flag.	option	-

Option	Description
<i>enable</i>	Enable honoring of Don't-Fragment flag.
<i>disable</i>	Disable honoring of Don't-Fragment flag.

Parameter	Description	Type	Size														
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														
hw-switch-ether-filter *	Enable/disable hardware filter for certain Ethernet packet types.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow only ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100)</td></tr><tr><td><i>disable</i></td><td>Allow all packet types.</td></tr></table>			Option	Description	<i>enable</i>	Allow only ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100)	<i>disable</i>	Allow all packet types.								
Option	Description																
<i>enable</i>	Allow only ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100)																
<i>disable</i>	Allow all packet types.																
igmp-state-limit	Maximum number of IGMP memberships (96 - 64000, default = 3200).	integer	Minimum value: 96 Maximum value: 128000														
internal-switch-speed *	Internal port speed.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>auto</td></tr><tr><td><i>1000full</i></td><td>1000M Full</td></tr><tr><td><i>100full</i></td><td>100M full.</td></tr><tr><td><i>100half</i></td><td>100M half.</td></tr><tr><td><i>10full</i></td><td>10M full.</td></tr><tr><td><i>10half</i></td><td>10M half.</td></tr></table>			Option	Description	<i>auto</i>	auto	<i>1000full</i>	1000M Full	<i>100full</i>	100M full.	<i>100half</i>	100M half.	<i>10full</i>	10M full.	<i>10half</i>	10M half.
Option	Description																
<i>auto</i>	auto																
<i>1000full</i>	1000M Full																
<i>100full</i>	100M full.																
<i>100half</i>	100M half.																
<i>10full</i>	10M full.																
<i>10half</i>	10M half.																
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295														
ip-src-port-range	IP source port range used for traffic originating from the FortiGate unit.	user	Not Specified														
ips-affinity *	Affinity setting for IPS (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).	string	Maximum length: 79														

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ASIC offload for IPsec VPN.</td></tr><tr><td><i>disable</i></td><td>Disable ASIC offload for IPsec VPN.</td></tr></table>	Option	Description	<i>enable</i>	Enable ASIC offload for IPsec VPN.	<i>disable</i>	Disable ASIC offload for IPsec VPN.		
Option	Description								
<i>enable</i>	Enable ASIC offload for IPsec VPN.								
<i>disable</i>	Disable ASIC offload for IPsec VPN.								
ipsec-hmac-offload *	Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable offload IPsec HMAC processing to hardware if possible.</td></tr><tr><td><i>disable</i></td><td>Disable offload IPsec HMAC processing to hardware.</td></tr></table>	Option	Description	<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.	<i>disable</i>	Disable offload IPsec HMAC processing to hardware.		
Option	Description								
<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.								
<i>disable</i>	Disable offload IPsec HMAC processing to hardware.								
ipsec-soft-dec-async	Enable/disable software decryption asynchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable software decryption asynchronization for IPsec VPN.</td></tr><tr><td><i>disable</i></td><td>Disable software decryption asynchronization for IPsec VPN.</td></tr></table>	Option	Description	<i>enable</i>	Enable software decryption asynchronization for IPsec VPN.	<i>disable</i>	Disable software decryption asynchronization for IPsec VPN.		
Option	Description								
<i>enable</i>	Enable software decryption asynchronization for IPsec VPN.								
<i>disable</i>	Disable software decryption asynchronization for IPsec VPN.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable probing of IPv6 address space through Anycast</td></tr><tr><td><i>disable</i></td><td>Disable probing of IPv6 address space through Anycast</td></tr></table>	Option	Description	<i>enable</i>	Enable probing of IPv6 address space through Anycast	<i>disable</i>	Disable probing of IPv6 address space through Anycast		
Option	Description								
<i>enable</i>	Enable probing of IPv6 address space through Anycast								
<i>disable</i>	Disable probing of IPv6 address space through Anycast								
language	GUI display language.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>english</i></td><td>English.</td></tr><tr><td><i>french</i></td><td>French.</td></tr></table>	Option	Description	<i>english</i>	English.	<i>french</i>	French.		
Option	Description								
<i>english</i>	English.								
<i>french</i>	French.								

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr><tr><td><i>portuguese</i></td><td>Portuguese.</td></tr><tr><td><i>japanese</i></td><td>Japanese.</td></tr><tr><td><i>trach</i></td><td>Traditional Chinese.</td></tr><tr><td><i>simch</i></td><td>Simplified Chinese.</td></tr><tr><td><i>korean</i></td><td>Korean.</td></tr></table>	Option	Description	<i>spanish</i>	Spanish.	<i>portuguese</i>	Portuguese.	<i>japanese</i>	Japanese.	<i>trach</i>	Traditional Chinese.	<i>simch</i>	Simplified Chinese.	<i>korean</i>	Korean.		
	Option	Description															
	<i>spanish</i>	Spanish.															
	<i>portuguese</i>	Portuguese.															
	<i>japanese</i>	Japanese.															
	<i>trach</i>	Traditional Chinese.															
	<i>simch</i>	Simplified Chinese.															
<i>korean</i>	Korean.																
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds (1 - 300000, default 500).	integer	Minimum value: 1 Maximum value: 300000														
legacy-poe-device-support *	Enable/disable legacy POE device support.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable legacy POE device support.</td></tr><tr><td><i>disable</i></td><td>Disable legacy POE device support.</td></tr></table>	Option	Description	<i>enable</i>	Enable legacy POE device support.	<i>disable</i>	Disable legacy POE device support.										
	Option	Description															
	<i>enable</i>	Enable legacy POE device support.															
<i>disable</i>	Disable legacy POE device support.																
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reception of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td><i>disable</i></td><td>Disable reception of Link Layer Discovery Protocol (LLDP).</td></tr></table>	Option	Description	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).										
	Option	Description															
	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).															
<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).																
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable transmission of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td><i>disable</i></td><td>Disable transmission of Link Layer Discovery Protocol (LLDP).</td></tr></table>	Option	Description	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).										
	Option	Description															
	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).															
<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).																
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging of SSL connection events.</td></tr><tr><td><i>disable</i></td><td>Disable logging of SSL connection events.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of SSL connection events.	<i>disable</i>	Disable logging of SSL connection events.										
	Option	Description															
	<i>enable</i>	Enable logging of SSL connection events.															
<i>disable</i>	Disable logging of SSL connection events.																

Parameter	Description	Type	Size						
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable insertion of address UUID to traffic logs.</td></tr><tr><td><i>disable</i></td><td>Disable insertion of address UUID to traffic logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable insertion of address UUID to traffic logs.	<i>disable</i>	Disable insertion of address UUID to traffic logs.		
Option	Description								
<i>enable</i>	Enable insertion of address UUID to traffic logs.								
<i>disable</i>	Disable insertion of address UUID to traffic logs.								
log-uuid-policy	Enable/disable insertion of policy UUIDs to traffic logs.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable insertion of policy UUID to traffic logs.</td></tr><tr><td><i>disable</i></td><td>Disable insertion of policy UUID to traffic logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable insertion of policy UUID to traffic logs.	<i>disable</i>	Disable insertion of policy UUID to traffic logs.		
Option	Description								
<i>enable</i>	Enable insertion of policy UUID to traffic logs.								
<i>disable</i>	Disable insertion of policy UUID to traffic logs.								
login-timestamp	Enable/disable login time recording.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable login time recording.</td></tr><tr><td><i>disable</i></td><td>Disable login time recording.</td></tr></table>	Option	Description	<i>enable</i>	Enable login time recording.	<i>disable</i>	Disable login time recording.		
Option	Description								
<i>enable</i>	Enable login time recording.								
<i>disable</i>	Disable login time recording.								
long-vdom-name *	Enable/disable long VDOM name support.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable long VDOM name support.</td></tr><tr><td><i>disable</i></td><td>Disable long VDOM name support.</td></tr></table>	Option	Description	<i>enable</i>	Enable long VDOM name support.	<i>disable</i>	Disable long VDOM name support.		
Option	Description								
<i>enable</i>	Enable long VDOM name support.								
<i>disable</i>	Disable long VDOM name support.								
management-vdom	Management virtual domain name.	string	Maximum length: 31						
max-dlpstat-memory	Maximum DLP stat memory (0 - 4294967295).	integer	Not Specified						
max-route-cache-size	Maximum number of IP route cache entries (0 - 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647						
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme (new sessions are dropped) (% of total RAM, default = 95).	integer	Minimum value: 70 Maximum value: 97						

Parameter	Description	Type	Size
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode (% of total RAM, default = 82).	integer	Minimum value: 70 Maximum value: 97
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode (% of total RAM, default = 88).	integer	Minimum value: 70 Maximum value: 97
miglog-affinity *	Affinity setting for logging (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 19
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
multi-factor-authentication	Enforce all login methods to require an additional authentication factor (default = optional).	option	-

Option	Description
<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).
<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.

ndp-max-entry	Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries).	integer	Minimum value: 65536 Maximum value: 2147483647
per-user-bwl *	Enable/disable per-user black/white list filter.	option	-

Option	Description
<i>enable</i>	Enable per-user black/white list filter.
<i>disable</i>	Disable per-user black/white list filter.

pmtu-discovery	Enable/disable path MTU discovery.	option	-

Option	Description
<i>enable</i>	Enable path MTU discovery.
<i>disable</i>	Disable path MTU discovery.

Parameter	Description	Type	Size						
policy-auth-concurrent	Number of concurrent firewall use logins from the same user (1 - 100, default = 0 means no limit).	integer	Minimum value: 0 Maximum value: 100						
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable post-login banner.</td></tr><tr><td><i>enable</i></td><td>Enable post-login banner.</td></tr></table>	Option	Description	<i>disable</i>	Disable post-login banner.	<i>enable</i>	Enable post-login banner.		
Option	Description								
<i>disable</i>	Disable post-login banner.								
<i>enable</i>	Enable post-login banner.								
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pre-login banner.</td></tr><tr><td><i>disable</i></td><td>Disable pre-login banner.</td></tr></table>	Option	Description	<i>enable</i>	Enable pre-login banner.	<i>disable</i>	Disable pre-login banner.		
Option	Description								
<i>enable</i>	Enable pre-login banner.								
<i>disable</i>	Disable pre-login banner.								
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable private data encryption using an AES 128-bit key.</td></tr><tr><td><i>enable</i></td><td>Enable private data encryption using an AES 128-bit key.</td></tr></table>	Option	Description	<i>disable</i>	Disable private data encryption using an AES 128-bit key.	<i>enable</i>	Enable private data encryption using an AES 128-bit key.		
Option	Description								
<i>disable</i>	Disable private data encryption using an AES 128-bit key.								
<i>enable</i>	Enable private data encryption using an AES 128-bit key.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authenticated users lifetime control.</td></tr><tr><td><i>disable</i></td><td>Disable authenticated users lifetime control.</td></tr></table>	Option	Description	<i>enable</i>	Enable authenticated users lifetime control.	<i>disable</i>	Disable authenticated users lifetime control.		
Option	Description								
<i>enable</i>	Enable authenticated users lifetime control.								
<i>disable</i>	Disable authenticated users lifetime control.								
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users (5 - 65535 min, default=480 (8 hours)).	integer	Minimum value: 5 Maximum value: 65535						

Parameter	Description	Type	Size								
proxy-auth-timeout	Authentication timeout in minutes for authenticated users (1 - 300 min, default = 10).	integer	Minimum value: 1 Maximum value: 300								
proxy-cipher-hardware-acceleration *	Enable/disable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.</td></tr><tr><td><i>enable</i></td><td>Enable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.	<i>enable</i>	Enable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.				
Option	Description										
<i>disable</i>	Disable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.										
<i>enable</i>	Enable using content processor (CP8 or CP9) hardware acceleration to encrypt and decrypt IPsec and SSL traffic.										
proxy-kxp-hardware-acceleration *	Enable/disable using the content processor to accelerate KXP traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable using the content processor to accelerate KXP traffic.</td></tr><tr><td><i>enable</i></td><td>Enable using the content processor to accelerate KXP traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable using the content processor to accelerate KXP traffic.	<i>enable</i>	Enable using the content processor to accelerate KXP traffic.				
Option	Description										
<i>disable</i>	Disable using the content processor to accelerate KXP traffic.										
<i>enable</i>	Enable using the content processor to accelerate KXP traffic.										
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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>session</i></td><td>Proxy re-authentication timeout begins at the closure of the session.</td></tr><tr><td><i>traffic</i></td><td>Proxy re-authentication timeout begins after traffic has not been received.</td></tr><tr><td><i>absolute</i></td><td>Proxy re-authentication timeout begins when the user was first created.</td></tr></table>	Option	Description	<i>session</i>	Proxy re-authentication timeout begins at the closure of the session.	<i>traffic</i>	Proxy re-authentication timeout begins after traffic has not been received.	<i>absolute</i>	Proxy re-authentication timeout begins when the user was first created.		
Option	Description										
<i>session</i>	Proxy re-authentication timeout begins at the closure of the session.										
<i>traffic</i>	Proxy re-authentication timeout begins after traffic has not been received.										
<i>absolute</i>	Proxy re-authentication timeout begins when the user was first created.										
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 8 **								
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535								
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-								

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable reboot of system upon restoring configuration.
<i>disable</i>	Disable reboot of system upon restoring configuration.

refresh	Statistics refresh interval in GUI.	integer	Minimum value: 0 Maximum value: 4294967295
remoteauthtimeout	Number of seconds that the FortiGate waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. (0-300 sec, default = 5, 0 means no timeout).	integer	Minimum value: 1 Maximum value: 300
reset-sessionless-tcp	Action to perform if the FortiGate receives a TCP packet but cannot find a corresponding session in its session table. NAT/Route mode only.	option	-

Option	Description
<i>enable</i>	Enable reset session-less TCP.
<i>disable</i>	Disable reset session-less TCP.

restart-time	Daily restart time (hh:mm).	user	Not Specified
revision-backup-on-logout *	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-

Option	Description
<i>enable</i>	Enable revision config backup automatically when logout.
<i>disable</i>	Disable revision config backup automatically when logout.

revision-image-auto-backup *	Enable/disable back-up of the latest configuration revision after the firmware is upgraded.	option	-

Option	Description
<i>enable</i>	Enable revision image backup automatically when upgrading image.
<i>disable</i>	Disable revision image backup automatically when upgrading image.

Parameter	Description	Type	Size
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: 8 **
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-

Option	Description
<i>enable</i>	Enable submission of Security Rating results to FortiGuard.
<i>disable</i>	Disable submission of Security Rating results to FortiGuard.

security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-

Option	Description
<i>enable</i>	Enable scheduled runs of Security Rating.
<i>disable</i>	Disable scheduled runs of Security Rating.

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
<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.
<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.

show-backplane-intf *	show/hide backplane interfaces	option	-

Option	Description
<i>enable</i>	show backplane interfaces
<i>disable</i>	hide backplane interfaces

snat-route-change	Enable/disable the ability to change the static NAT route.	option	-

Option	Description
<i>enable</i>	Enable SNAT route change.
<i>disable</i>	Disable SNAT route change.

Parameter	Description	Type	Size												
special-file-23-support	Enable/disable IPS detection of HIBUN format files when using Data Leak Protection.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable using IPS detection of HIBUN format files when using Data Leak Protection.</td></tr><tr><td>enable</td><td>Enable using IPS detection of HIBUN format files when using Data Leak Protection.</td></tr></table>			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.						
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.														
split-port *	Split port(s) to multiple 10Gbps ports.	user	Not Specified												
ssd-trim-date *	Date within a month to run ssd trim.	integer	Minimum value: 1 Maximum value: 31												
ssd-trim-freq *	How often to run SSD Trim (default = weekly). SSD Trim prevents SSD drive data loss by finding and isolating errors.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>never</td><td>Never Run SSD Trim.</td></tr><tr><td>hourly</td><td>Run SSD Trim Hourly.</td></tr><tr><td>daily</td><td>Run SSD Trim Daily.</td></tr><tr><td>weekly</td><td>Run SSD Trim Weekly.</td></tr><tr><td>monthly</td><td>Run SSD Trim Monthly.</td></tr></table>			Option	Description	never	Never Run SSD Trim.	hourly	Run SSD Trim Hourly.	daily	Run SSD Trim Daily.	weekly	Run SSD Trim Weekly.	monthly	Run SSD Trim Monthly.
Option	Description														
never	Never Run SSD Trim.														
hourly	Run SSD Trim Hourly.														
daily	Run SSD Trim Daily.														
weekly	Run SSD Trim Weekly.														
monthly	Run SSD Trim Monthly.														
ssd-trim-hour *	Hour of the day on which to run SSD Trim (0 - 23, default = 1).	integer	Minimum value: 0 Maximum value: 23												
ssd-trim-min *	Minute of the hour on which to run SSD Trim (0 - 59, 60 for random).	integer	Minimum value: 0 Maximum value: 60												
ssd-trim-weekday *	Day of week to run SSD Trim.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sunday</td><td>Sunday</td></tr><tr><td>monday</td><td>Monday</td></tr></table>			Option	Description	sunday	Sunday	monday	Monday						
Option	Description														
sunday	Sunday														
monday	Monday														

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tuesday</i></td><td>Tuesday</td></tr><tr><td><i>wednesday</i></td><td>Wednesday</td></tr><tr><td><i>thursday</i></td><td>Thursday</td></tr><tr><td><i>friday</i></td><td>Friday</td></tr><tr><td><i>saturday</i></td><td>Saturday</td></tr></table>	Option	Description	<i>tuesday</i>	Tuesday	<i>wednesday</i>	Wednesday	<i>thursday</i>	Thursday	<i>friday</i>	Friday	<i>saturday</i>	Saturday		
	Option	Description													
	<i>tuesday</i>	Tuesday													
	<i>wednesday</i>	Wednesday													
	<i>thursday</i>	Thursday													
	<i>friday</i>	Friday													
	<i>saturday</i>	Saturday													
ssh-cbc-cipher	Enable/disable CBC cipher for SSH access.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable CBC cipher for SSH access.</td></tr><tr><td><i>disable</i></td><td>Disable CBC cipher for SSH access.</td></tr></table>	Option	Description	<i>enable</i>	Enable CBC cipher for SSH access.	<i>disable</i>	Disable CBC cipher for SSH access.								
	Option	Description													
	<i>enable</i>	Enable CBC cipher for SSH access.													
<i>disable</i>	Disable CBC cipher for SSH access.														
ssh-hmac-md5	Enable/disable HMAC-MD5 for SSH access.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HMAC-MD5 for SSH access.</td></tr><tr><td><i>disable</i></td><td>Disable HMAC-MD5 for SSH access.</td></tr></table>	Option	Description	<i>enable</i>	Enable HMAC-MD5 for SSH access.	<i>disable</i>	Disable HMAC-MD5 for SSH access.								
	Option	Description													
	<i>enable</i>	Enable HMAC-MD5 for SSH access.													
<i>disable</i>	Disable HMAC-MD5 for SSH access.														
ssh-kex-sha1	Enable/disable SHA1 key exchange for SSH access.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SHA1 for SSH key exchanges.</td></tr><tr><td><i>disable</i></td><td>Disable SHA1 for SSH key exchanges.</td></tr></table>	Option	Description	<i>enable</i>	Enable SHA1 for SSH key exchanges.	<i>disable</i>	Disable SHA1 for SSH key exchanges.								
	Option	Description													
	<i>enable</i>	Enable SHA1 for SSH key exchanges.													
<i>disable</i>	Disable SHA1 for SSH key exchanges.														
ssh-mac-weak	Enable/disable HMAC-SHA1 and UMAC-64-ETM for SSH access.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.</td></tr><tr><td><i>disable</i></td><td>Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.</td></tr></table>	Option	Description	<i>enable</i>	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.	<i>disable</i>	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.								
	Option	Description													
	<i>enable</i>	Enable HMAC-SHA1 and UMAC-64-ETM for SSH access.													
<i>disable</i>	Disable HMAC-SHA1 and UMAC-64-ETM for SSH access.														
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default = TLSv1.2).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr></table>	Option	Description	SSLv3	SSLv3.										
	Option	Description													
SSLv3	SSLv3.														

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.		
Option	Description												
<i>TLSv1</i>	TLSv1.												
<i>TLSv1-1</i>	TLSv1.1.												
<i>TLSv1-2</i>	TLSv1.2.												
<i>TLSv1-3</i>	TLSv1.3.												
ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable static key ciphers in SSL/TLS connections.</td></tr><tr><td><i>disable</i></td><td>Disable static key ciphers in SSL/TLS connections.</td></tr></table>	Option	Description	<i>enable</i>	Enable static key ciphers in SSL/TLS connections.	<i>disable</i>	Disable static key ciphers in SSL/TLS connections.						
Option	Description												
<i>enable</i>	Enable static key ciphers in SSL/TLS connections.												
<i>disable</i>	Disable static key ciphers in SSL/TLS connections.												
sslvpn-cipher-hardware-acceleration *	Enable/disable SSL VPN hardware acceleration.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN cipher hardware acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN cipher hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.	<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.						
Option	Description												
<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.												
<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.												
sslvpn-kxp-hardware-acceleration *	Enable/disable SSL VPN KXP hardware acceleration.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable KXP SSL-VPN hardware acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable KXP SSL-VPN hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable KXP SSL-VPN hardware acceleration.	<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.						
Option	Description												
<i>enable</i>	Enable KXP SSL-VPN hardware acceleration.												
<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.												
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: 8 **										
sslvpn-plugin-version-check	Enable/disable checking browser's plugin version by SSL VPN.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN automatic checking of browser plug-in version.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN automatic checking of browser plug-in version.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.	<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.						
Option	Description												
<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.												
<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.												

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict dirty-session check.</td></tr><tr><td><i>disable</i></td><td>Disable strict dirty-session check.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict dirty-session check.	<i>disable</i>	Disable strict dirty-session check.		
Option	Description								
<i>enable</i>	Enable strict dirty-session check.								
<i>disable</i>	Disable strict dirty-session check.								
strong-crypto	Enable to use strong encryption and only allow strong ciphers (AES) and digest (SHA1) for HTTPS/SSH/TLS/SSL functions.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr><tr><td><i>disable</i></td><td>Disable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr></table>	Option	Description	<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.	<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.		
Option	Description								
<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.								
<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.								
switch-controller *	Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable switch controller feature.</td></tr><tr><td><i>enable</i></td><td>Enable switch controller feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable switch controller feature.	<i>enable</i>	Enable switch controller feature.		
Option	Description								
<i>disable</i>	Disable switch controller feature.								
<i>enable</i>	Enable switch controller feature.								
switch-controller-reserved-network *	Enable reserved network subnet for controlled switches. This is available when the switch controller is enabled.	ipv4-classnet	Not Specified						
sys-perf-log-interval	Time in minutes between updates of performance statistics logging. (1 - 15 min, default = 5, 0 = disabled).	integer	Minimum value: 0 Maximum value: 15						
tcp-halfclose-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded (1 - 86400 sec (1 day), default = 120).	integer	Minimum value: 1 Maximum value: 86400						

Parameter	Description	Type	Size
tcp-halfopen-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded (1 - 86400 sec (1 day), default = 10).	integer	Minimum value: 1 Maximum value: 86400
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-

Option	Description
<i>enable</i>	Enable TCP option.
<i>disable</i>	Disable TCP option.

tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300
tftp	Enable/disable TFTP.	option	-

Option	Description
<i>enable</i>	Enable TFTP.
<i>disable</i>	Disable TFTP.

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)

Parameter	Description	Type	Size

Option	Description
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
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

Parameter	Description	Type	Size

Option	Description
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
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

Parameter	Description	Type	Size

Option	Description
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
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
<i>tos</i>	IP TOS.
<i>dscp</i>	DSCP (DiffServ) DS.

traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-

Parameter	Description	Type	Size

	Option	Description		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		

two-factor-email-expiry	Email-based two-factor authentication session timeout (30 - 300 seconds (5 minutes), default = 60).	integer	Minimum value: 30 Maximum value: 300
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout (10 - 3600 seconds (1 hour), default = 60).	integer	Minimum value: 10 Maximum value: 3600
two-factor-ftk-expiry	FortiToken authentication session timeout (60 - 600 sec (10 minutes), default = 60).	integer	Minimum value: 60 Maximum value: 600
two-factor-ftm-expiry	FortiToken Mobile session timeout (1 - 168 hours (7 days), default = 72).	integer	Minimum value: 1 Maximum value: 168
two-factor-sms-expiry	SMS-based two-factor authentication session timeout (30 - 300 sec, default = 60).	integer	Minimum value: 30 Maximum value: 300
udp-idle-timer	UDP connection session timeout. This command can be useful in managing CPU and memory resources (1 - 86400 seconds (1 day), default = 60).	integer	Minimum value: 1 Maximum value: 86400
url-filter-affinity *	URL filter CPU affinity.	string	Maximum length: 79
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1 **
user-server-cert	Certificate to use for https user authentication.	string	Maximum length: 35
vdom-mode *	Enable/disable support for split/multiple virtual domains (VDOMs).	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>no-vdom</i>	Disable split/multiple VDOMs mode.	
	<i>split-vdom</i>	Enable split VDOMs mode.	
	<i>multi-vdom</i>	Enable multiple VDOMs mode.	
vip-arp-range	Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.	option	-
	Option	Description	
	<i>unlimited</i>	Send ARPs for all addresses in VIP range.	
	<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.	
virtual-switch-vlan *	Enable/disable virtual switch VLAN.	option	-
	Option	Description	
	<i>enable</i>	Enable virtual switch VLAN.	
	<i>disable</i>	Disable virtual switch VLAN.	
wad-affinity *	Affinity setting for wad (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 8 **
wad-memory-change-granularity	Minimum percentage change in system memory usage detected by the wad daemon prior to adjusting TCP window size for any active connection.	integer	Minimum value: 5 Maximum value: 25
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-
	Option	Description	
	<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.	
	<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.	

Parameter	Description	Type	Size
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: 8 **
wifi-ca-certificate	CA certificate that verifies the WiFi certificate.	string	Maximum length: 79
wifi-certificate	Certificate to use for WiFi authentication.	string	Maximum length: 35
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-

Option	Description
<i>enable</i>	Enable WiMax 4G.
<i>disable</i>	Disable WiMax 4G.

wireless-controller	Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.	option	-

Option	Description
<i>enable</i>	Enable wireless controller.
<i>disable</i>	Disable wireless controller.

wireless-controller-port	Port used for the control channel in wireless controller mode (wireless-mode is ac). The data channel port is the control channel port number plus one (1024 - 49150, default = 5246).	integer	Minimum value: 1024 Maximum value: 49150
wireless-mode *	Wireless mode setting.	option	-

Option	Description
<i>ac</i>	Wireless controller with local wireless.
<i>client</i>	Wireless client mode.
<i>fwfap</i>	Obsolete wireless AP mode.

* This parameter may not exist in some models.

** Values may differ between models.

config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set checksum-reception [disable|enable]
    set checksum-transmission [disable|enable]
    set diffservcode {user}
    set dscp-copying [disable|enable]
    set interface {string}
    set ip-version [4|6]
    set keepalive-failtimes {integer}
    set keepalive-interval {integer}
    set key-inbound {integer}
    set key-outbound {integer}
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set sequence-number-reception [disable|enable]
    set sequence-number-transmission [disable|enable]
  next
end
```

config system gre-tunnel

Parameter	Description	Type	Size
checksum-reception *	Enable/disable validating checksums in received GRE packets.	option	-
	Option	Description	
	<i>disable</i>	Do not validate checksums in received GRE packets.	
	<i>enable</i>	Validate checksums in received GRE packets.	
checksum-transmission *	Enable/disable including checksums in transmitted GRE packets.	option	-
	Option	Description	
	<i>disable</i>	Do not include checksums in transmitted GRE packets.	
	<i>enable</i>	Include checksums in transmitted GRE packets.	
diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified
dscp-copying	Enable/disable DSCP copying.	option	-

Parameter	Description	Type	Size

Option	Description
<i>disable</i>	Disable DSCP copying.
<i>enable</i>	Enable DSCP copying.

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.

keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down (1 - 255).	integer	Minimum value: 1 Maximum value: 255
keepalive-interval	Keepalive message interval (0 - 32767, 0 = disabled).	integer	Minimum value: 0 Maximum value: 32767
key-inbound *	Require received GRE packets contain this key (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
key-outbound *	Include this key in transmitted GRE packets (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified
local-gw6	IPv6 address of the local gateway.	ipv6-address	Not Specified
name	Tunnel name.	string	Maximum length: 15
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified
remote-gw6	IPv6 address of the remote gateway.	ipv6-address	Not Specified

Parameter	Description	Type	Size						
sequence-number-reception *	Enable/disable validating sequence numbers in received GRE packets.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not validate sequence number in received GRE packets.</td></tr><tr><td><i>enable</i></td><td>Validate sequence numbers in received GRE packets.</td></tr></table>	Option	Description	<i>disable</i>	Do not validate sequence number in received GRE packets.	<i>enable</i>	Validate sequence numbers in received GRE packets.		
Option	Description								
<i>disable</i>	Do not validate sequence number in received GRE packets.								
<i>enable</i>	Validate sequence numbers in received GRE packets.								
sequence-number-transmission *	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Include sequence numbers in transmitted GRE packets.</td></tr><tr><td><i>enable</i></td><td>Do not include sequence numbers in transmitted GRE packets.</td></tr></table>	Option	Description	<i>disable</i>	Include sequence numbers in transmitted GRE packets.	<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.		
Option	Description								
<i>disable</i>	Include sequence numbers in transmitted GRE packets.								
<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.								

* This parameter may not exist in some models.

config system ha

Configure HA.

```
config system ha
    Description: Configure HA.
    set arps {integer}
    set arps-interval {integer}
    set authentication [enable|disable]
    set cpu-threshold {user}
    set encryption [enable|disable]
    set frup [enable|disable]
    config frup-settings
        Description: FRUP settings
        set active-interface <name1>, <name2>, ...
        set active-switch-port {option1}, {option2}, ...
        set backup-interface <name1>, <name2>, ...
    end
    set ftp-proxy-threshold {user}
    set gratuitous-arps [enable|disable]
    set group-id {integer}
    set group-name {string}
    set ha-direct [enable|disable]
    set ha-eth-type {string}
    config ha-mgmt-interfaces
        Description: Reserve interfaces to manage individual cluster units.
        edit <id>
            set dst {ipv4-classnet}
            set gateway {ipv4-address}
            set gateway6 {ipv6-address}
```

```

        set interface {string}
    next
end
set ha-mgmt-status [enable|disable]
set ha-uptime-diff-margin {integer}
set hb-interval {integer}
set hb-lost-threshold {integer}
set hbdev {user}
set hc-eth-type {string}
set hello-holddown {integer}
set http-proxy-threshold {user}
set imap-proxy-threshold {user}
set inter-cluster-session-sync [enable|disable]
set key {password}
set l2ep-eth-type {string}
set link-failed-signal [enable|disable]
set load-balance-all [enable|disable]
set logical-sn [enable|disable]
set memory-compatible-mode [enable|disable]
set memory-threshold {user}
set minimum-worker-threshold {integer}
set mode [standalone|a-a|...]
set monitor {user}
set multicast-ttl {integer}
set nntp-proxy-threshold {user}
set override [enable|disable]
set override-wait-time {integer}
set password {password}
set pingserver-failover-threshold {integer}
set pingserver-flip-timeout {integer}
set pingserver-monitor-interface {user}
set pingserver-slave-force-reset [enable|disable]
set pop3-proxy-threshold {user}
set priority {integer}
set route-hold {integer}
set route-ttl {integer}
set route-wait {integer}
set schedule [none|hub|...]
config secondary-vcluster
    Description: Configure virtual cluster 2.
    set monitor {user}
    set override [enable|disable]
    set override-wait-time {integer}
    set pingserver-failover-threshold {integer}
    set pingserver-monitor-interface {user}
    set pingserver-slave-force-reset [enable|disable]
    set priority {integer}
    set vcluster-id {integer}
    set vdom {user}
end
set session-pickup [enable|disable]
set session-pickup-connectionless [enable|disable]
set session-pickup-delay [enable|disable]
set session-pickup-expectation [enable|disable]
set session-pickup-nat [enable|disable]
set session-sync-dev {user}

```

```

set slave-switch-standby [enable|disable]
set smtp-proxy-threshold {user}
set ssd-failover [enable|disable]
set standalone-config-sync [enable|disable]
set standalone-mgmt-vdom [enable|disable]
set sync-config [enable|disable]
set sync-packet-balance [enable|disable]
set unicast-hb [enable|disable]
set unicast-hb-netmask {ipv4-netmask}
set unicast-hb-peerip {ipv4-address}
set uninterruptible-upgrade [enable|disable]
set vcluster-id {integer}
set vcluster2 [enable|disable]
set vdom {user}
set weight {user}

```

end

config system ha

Parameter	Description	Type	Size						
arps	Number of gratuitous ARPs (1 - 60). Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60						
arps-interval	Time between gratuitous ARPs (1 - 20 sec). Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20						
authentication	Enable/disable heartbeat message authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable heartbeat message authentication.</td></tr><tr><td><i>disable</i></td><td>Disable heartbeat message authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable heartbeat message authentication.	<i>disable</i>	Disable heartbeat message authentication.		
Option	Description								
<i>enable</i>	Enable heartbeat message authentication.								
<i>disable</i>	Disable heartbeat message authentication.								
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified						
encryption	Enable/disable heartbeat message encryption.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable heartbeat message encryption.</td></tr><tr><td><i>disable</i></td><td>Disable heartbeat message encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable heartbeat message encryption.	<i>disable</i>	Disable heartbeat message encryption.		
Option	Description								
<i>enable</i>	Enable heartbeat message encryption.								
<i>disable</i>	Disable heartbeat message encryption.								
frup *	Enable/disable Fortinet Redundant UTM Protocol	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified						
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable gratuitous ARPs.</td></tr><tr><td><i>disable</i></td><td>Disable gratuitous ARPs.</td></tr></table>	Option	Description	<i>enable</i>	Enable gratuitous ARPs.	<i>disable</i>	Disable gratuitous ARPs.		
	Option	Description							
	<i>enable</i>	Enable gratuitous ARPs.							
<i>disable</i>	Disable gratuitous ARPs.								
group-id	Cluster group ID (0 - 255). 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						
ha-direct	Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, and FortiSandbox.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.</td></tr><tr><td><i>disable</i></td><td>Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.</td></tr></table>	Option	Description	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.	<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.		
	Option	Description							
	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.							
<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiManager and FortiSandbox.								
ha-eth-type	HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4						
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size						
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535						
hb-interval	Time between sending heartbeat packets (1 - 20 (100*ms)). Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20						
hb-lost-threshold	Number of lost heartbeats to signal a failure (1 - 60). Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60						
hbdev	Heartbeat interfaces. Must be the same for all members. Enter <interface> <priority> pairs to specify the priority of each heartbeat interface. Higher priority takes precedence.	user	Not Specified						
hc-eth-type	Transparent mode HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4						
hello-holddown	Time to wait before changing from hello to work state (5 - 300 sec).	integer	Minimum value: 5 Maximum value: 300						
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified						
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified						
inter-cluster-session-sync	Enable/disable synchronization of sessions among HA clusters.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization of sessions among HA clusters.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization of sessions among HA clusters.</td></tr></table>	Option	Description	<i>enable</i>	Enable synchronization of sessions among HA clusters.	<i>disable</i>	Disable synchronization of sessions among HA clusters.		
Option	Description								
<i>enable</i>	Enable synchronization of sessions among HA clusters.								
<i>disable</i>	Disable synchronization of sessions among HA clusters.								
key	key	password	Not Specified						
l2ep-eth-type	Telnet session HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4						
link-failed-signal	Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-
	Option	Description	
	<i>enable</i>	Enable load balance.	
	<i>disable</i>	Disable load balance.	
logical-sn	Enable/disable usage of the logical serial number.	option	-
	Option	Description	
	<i>enable</i>	Enable usage of the logical serial number.	
	<i>disable</i>	Disable usage of the logical serial number.	
memory-compatible-mode	Enable/disable memory compatible mode.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified
minimum-worker-threshold *	The minimum number of operating workers to cause a content clustering chassis failover.	integer	Minimum value: 1 Maximum value: 11
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-
	Option	Description	
	<i>standalone</i>	Standalone mode.	
	<i>a-a</i>	Active-active mode.	
	<i>a-p</i>	Active-passive mode.	

Parameter	Description	Type	Size
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified
multicast-ttl	HA multicast TTL on master (5 - 3600 sec).	integer	Minimum value: 5 Maximum value: 3600
nntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified
override	Enable and increase the priority of the unit that should always be primary (master).	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

override-wait-time	Delay negotiating if override is enabled (0 - 3600 sec). Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600
password	Cluster password. Must be the same for all members.	password	Not Specified
pingserver-failover-threshold	Remote IP monitoring failover threshold (0 - 50).	integer	Minimum value: 0 Maximum value: 50
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified
pingserver-slave-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-

Option	Description
<i>enable</i>	Enable force reset of slave after PING server failure.
<i>disable</i>	Disable force reset of slave after PING server failure.

Parameter	Description	Type	Size
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified
priority	Increase the priority to select the primary unit (0 - 255).	integer	Minimum value: 0 Maximum value: 255
route-hold	Time to wait between routing table updates to the cluster (0 - 3600 sec).	integer	Minimum value: 0 Maximum value: 3600
route-ttl	TTL for primary unit routes (5 - 3600 sec). 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 (0 - 3600 sec).	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
<i>none</i>	None.
<i>hub</i>	Hub.
<i>leastconnection</i>	Least connection.
<i>round-robin</i>	Round robin.
<i>weight-round-robin</i>	Weight round robin.
<i>random</i>	Random.
<i>ip</i>	IP.
<i>ipport</i>	IP port.

session-pickup	Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.	option	-

Option	Description
<i>enable</i>	Enable session pickup.
<i>disable</i>	Disable session pickup.

Parameter	Description	Type	Size						
session-pickup-connectionless	Enable/disable UDP and ICMP session sync.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
session-pickup-delay	Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
session-pickup-expectation	Enable/disable session helper expectation session sync for FGSP.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
session-pickup-nat	Enable/disable NAT session sync for FGSP.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified						
slave-switch-standby *	Enable to force content clustering subordinate unit standby mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>enable</td></tr><tr><td><i>disable</i></td><td>disable</td></tr></table>	Option	Description	<i>enable</i>	enable	<i>disable</i>	disable		
Option	Description								
<i>enable</i>	enable								
<i>disable</i>	disable								
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified						
ssd-failover	Enable/disable automatic HA failover on SSD disk failure.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
standalone-config-sync	Enable/disable FGSP configuration synchronization.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
standalone-mgmt-vdom	Enable/disable standalone management VDOM.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
sync-config	Enable/disable configuration synchronization.	option	-
	Option	Description	
	<i>enable</i>	Enable configuration synchronization.	
	<i>disable</i>	Disable configuration synchronization.	
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-
	Option	Description	
	<i>enable</i>	Enable HA packet distribution to multiple CPUs.	
	<i>disable</i>	Disable HA packet distribution to multiple CPUs.	
unicast-hb *	Enable/disable unicast heartbeat.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
unicast-hb-netmask *	Unicast heartbeat netmask.	ipv4-netmask	Not Specified

Parameter	Description	Type	Size						
unicast-hb-peerip *	Unicast heartbeat peer IP.	ipv4-address	Not Specified						
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
vcluster-id	Cluster ID. Read-only.	integer	Minimum value: 0 Maximum value: 255						
vcluster2	Enable/disable virtual cluster 2 for virtual clustering.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
vdom	VDOMs in virtual cluster 1.	user	Not Specified						
weight	Weight-round-robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified						

* This parameter may not exist in some models.

config frup-settings

Parameter	Description	Type	Size
active-interface <name>	FRUP active interface Interface name.	string	Maximum length: 15
active-switch- port	FRUP active switch port list	option	-
	Option	Description	
	1	switch port number	
	2	switch port number	
	3	switch port number	
	4	switch port number	

Parameter	Description	Type	Size																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5</td><td>switch port number</td></tr><tr><td>6</td><td>switch port number</td></tr><tr><td>7</td><td>switch port number</td></tr><tr><td>8</td><td>switch port number</td></tr><tr><td>9</td><td>switch port number</td></tr><tr><td>10</td><td>switch port number</td></tr><tr><td>11</td><td>switch port number</td></tr><tr><td>12</td><td>switch port number</td></tr><tr><td>13</td><td>switch port number</td></tr><tr><td>14</td><td>switch port number</td></tr><tr><td>15</td><td>switch port number</td></tr><tr><td>16</td><td>switch port number</td></tr></table>	Option	Description	5	switch port number	6	switch port number	7	switch port number	8	switch port number	9	switch port number	10	switch port number	11	switch port number	12	switch port number	13	switch port number	14	switch port number	15	switch port number	16	switch port number		
	Option	Description																											
	5	switch port number																											
	6	switch port number																											
	7	switch port number																											
	8	switch port number																											
	9	switch port number																											
	10	switch port number																											
	11	switch port number																											
	12	switch port number																											
	13	switch port number																											
	14	switch port number																											
	15	switch port number																											
16	switch port number																												
backup-interface <name>	FRUP backup interface Interface name.	string	Maximum length: 15																										

config ha-mgmt-interfaces

Parameter	Description	Type	Size
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
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Interface to reserve for HA management.	string	Maximum length: 15

config secondary-vcluster

Parameter	Description	Type	Size						
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified						
override	Enable and increase the priority of the unit that should always be primary (master).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
override-wait-time	Delay negotiating if override is enabled (0 - 3600 sec). Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600						
pingserver-failover-threshold	Remote IP monitoring failover threshold (0 - 50).	integer	Minimum value: 0 Maximum value: 50						
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified						
pingserver-slave-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable force reset of slave after PING server failure.</td></tr><tr><td><i>disable</i></td><td>Disable force reset of slave after PING server failure.</td></tr></table>			Option	Description	<i>enable</i>	Enable force reset of slave after PING server failure.	<i>disable</i>	Disable force reset of slave after PING server failure.
	Option	Description							
	<i>enable</i>	Enable force reset of slave after PING server failure.							
<i>disable</i>	Disable force reset of slave after PING server failure.								
priority	Increase the priority to select the primary unit (0 - 255).	integer	Minimum value: 0 Maximum value: 255						
vcluster-id	Cluster ID. Read-only.	integer	Minimum value: 0 Maximum value: 255						
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	
	<i>enable</i>	Enable monitor VLAN interfaces.	
	<i>disable</i>	Disable monitor VLAN interfaces.	
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30
vlan-hb-lost-threshold	VLAN lost heartbeat threshold (1 - 60).	integer	Minimum value: 1 Maximum value: 60

config system interface

Configure interfaces.

```
config system interface
    Description: Configure interfaces.
    edit <name>
        set ac-name {string}
        set aggregate {string}
        set algorithm [L2|L3|...]
        set alias {string}
        set allowaccess {option1}, {option2}, ...
        set ap-discover [enable|disable]
        set arpforward [enable|disable]
        set atm-protocol [none|ipoa]
        set auth-type [auto|pap|...]
        set auto-auth-extension-device [enable|disable]
        set bfd [global|enable|...]
```

```

set bfd-desired-min-tx {integer}
set bfd-detect-mult {integer}
set bfd-required-min-rx {integer}
set broadcast-forticlient-discovery [enable|disable]
set broadcast-forward [enable|disable]
set cli-conn-status {integer}
set color {integer}
set dedicated-to [none|management]
set defaultgw [enable|disable]
set description {var-string}
set detected-peer-mtu {integer}
set detectprotocol {option1}, {option2}, ...
set detectserver {user}
set device-identification [enable|disable]
set device-user-identification [enable|disable]
set devindex {integer}
set dhcp-client-identifier {string}
set dhcp-relay-agent-option [enable|disable]
set dhcp-relay-interface {string}
set dhcp-relay-interface-select-method [auto|sdwan|...]
set dhcp-relay-ip {user}
set dhcp-relay-request-all-server [disable|enable]
set dhcp-relay-service [disable|enable]
set dhcp-relay-type [regular|ipsec]
set dhcp-renew-time {integer}
set disc-retry-timeout {integer}
set disconnect-threshold {integer}
set distance {integer}
set dns-server-override [enable|disable]
set drop-fragment [enable|disable]
set drop-overlapped-fragment [enable|disable]
set egress-cos [disable|cos0|...]
config egress-queues
    Description: Configure queues of NP port on egress path.
    set cos0 {string}
    set cos1 {string}
    set cos2 {string}
    set cos3 {string}
    set cos4 {string}
    set cos5 {string}
    set cos6 {string}
    set cos7 {string}
end
set egress-shaping-profile {string}
set estimated-downstream-bandwidth {integer}
set estimated-upstream-bandwidth {integer}
set explicit-ftp-proxy [enable|disable]
set explicit-web-proxy [enable|disable]
set external [enable|disable]
set fail-action-on-extender [soft-restart|hard-restart|...]
set fail-alert-interfaces <name1>, <name2>, ...
set fail-alert-method [link-failed-signal|link-down]
set fail-detect [enable|disable]
set fail-detect-option {option1}, {option2}, ...
set fortilink [enable|disable]
set fortilink-backup-link {integer}

```

```

set fortilink-neighbor-detect [lldp|fortilink]
set fortilink-split-interface [enable|disable]
set fortilink-stacking [enable|disable]
set forward-domain {integer}
set forward-error-correction [enable|disable]
set gateway-address {ipv4-address}
set gwaddr {ipv4-address}
set gwdetect [enable|disable]
set ha-priority {integer}
set icmp-accept-redirect [enable|disable]
set icmp-send-redirect [enable|disable]
set ident-accept [enable|disable]
set idle-timeout {integer}
set inbandwidth {integer}
set ingress-cos [disable|cos0|...]
set ingress-shaping-profile {string}
set ingress-spillover-threshold {integer}
set interface {string}
set internal {integer}
set ip {ipv4-classnet-host}
set ipmac [enable|disable]
set ips-sniffer-mode [enable|disable]
set ipunnumbered {ipv4-address}
config ipv6
    Description: IPv6 of interface.
    set autoconf [enable|disable]
    set dhcp6-client-options {option1}, {option2}, ...
    set dhcp6-information-request [enable|disable]
    set dhcp6-prefix-delegation [enable|disable]
    set dhcp6-prefix-hint {ipv6-network}
    set dhcp6-prefix-hint-plt {integer}
    set dhcp6-prefix-hint-vlt {integer}
    set dhcp6-relay-ip {user}
    set dhcp6-relay-service [disable|enable]
    set dhcp6-relay-type {option}
    set ip6-address {ipv6-prefix}
    set ip6-allowaccess {option1}, {option2}, ...
    set ip6-default-life {integer}
    config ip6-delegated-prefix-list
        Description: Advertised IPv6 delegated prefix list.
        edit <prefix-id>
            set autonomous-flag [enable|disable]
            set onlink-flag [enable|disable]
            set rdns {user}
            set rdns-service [delegated|default|...]
            set subnet {ipv6-network}
            set upstream-interface {string}
        next
    end
    set ip6-dns-server-override [enable|disable]
    config ip6-extra-addr
        Description: Extra IPv6 address prefixes of interface.
        edit <prefix>
            next
        end
    set ip6-hop-limit {integer}

```

```

set ip6-link-mtu {integer}
set ip6-manage-flag [enable|disable]
set ip6-max-interval {integer}
set ip6-min-interval {integer}
set ip6-mode [static|dhcp|...]
set ip6-other-flag [enable|disable]
config ip6-prefix-list
    Description: Advertised prefix list.
    edit <prefix>
        set autonomous-flag [enable|disable]
        set dnssl <domain1>, <domain2>, ...
        set onlink-flag [enable|disable]
        set preferred-life-time {integer}
        set rdns {user}
        set valid-life-time {integer}
    next
end
set ip6-reachable-time {integer}
set ip6-retrans-time {integer}
set ip6-send-adv [enable|disable]
set ip6-subnet {ipv6-prefix}
set ip6-upstream-interface {string}
set nd-cert {string}
set nd-cga-modifier {user}
set nd-mode [basic|SEND-compatible]
set nd-security-level {integer}
set nd-timestamp-delta {integer}
set nd-timestamp-fuzz {integer}
set vrip6_link_local {ipv6-address}
set vrrp-virtual-mac6 [enable|disable]
config vrrp6
    Description: IPv6 VRRP configuration.
    edit <vrid>
        set accept-mode [enable|disable]
        set adv-interval {integer}
        set preempt [enable|disable]
        set priority {integer}
        set start-time {integer}
        set status [enable|disable]
        set vrdest6 {ipv6-address}
        set vrgrp {integer}
        set vrip6 {ipv6-address}
    next
end
end
set l2forward [enable|disable]
set l2tp-client [enable|disable]
config l2tp-client-settings
    Description: L2TP client settings.
    set auth-type [auto|pap|...]
    set defaultgw [enable|disable]
    set distance {integer}
    set ip {ipv4-classnet-host}
    set mtu {integer}
    set password {password}
    set peer-host {string}

```

```

        set peer-mask {ipv4-netmask}
        set peer-port {integer}
        set priority {integer}
        set user {string}
    end
    set lacp-ha-slave [enable|disable]
    set lacp-mode [static|passive|...]
    set lacp-speed [slow|fast]
    set lcp-echo-interval {integer}
    set lcp-max-echo-fails {integer}
    set link-up-delay {integer}
    set lldp-network-policy {string}
    set lldp-reception [enable|disable|...]
    set lldp-transmission [enable|disable|...]
    set macaddr {mac-address}
    set management-ip {ipv4-classnet-host}
    set mediatype [serdes-sfp|sgmii-sfp|...]
    set member <interface-name1>, <interface-name2>, ...
    set min-links {integer}
    set min-links-down [operational|administrative]
    set mode [static|dhcp|...]
    set mtu {integer}
    set mtu-override [enable|disable]
    set mux-type [llc-encaps|vc-encaps]
    set ndiscforward [enable|disable]
    set netbios-forward [disable|enable]
    set netflow-sampler [disable|tx|...]
    set outbandwidth {integer}
    set padt-retry-timeout {integer}
    set password {password}
    set phy-mode [adsl|vdsl]
    set ping-serv-status {integer}
    set poe [enable|disable]
    set polling-interval {integer}
    set ppoe-unnumbered-negotiate [enable|disable]
    set pptp-auth-type [auto|pap|...]
    set pptp-client [enable|disable]
    set pptp-password {password}
    set pptp-server-ip {ipv4-address}
    set pptp-timeout {integer}
    set pptp-user {string}
    set preserve-session-route [enable|disable]
    set priority {integer}
    set priority-override [enable|disable]
    set proxy-captive-portal [enable|disable]
    set redundant-interface {string}
    set remote-ip {ipv4-classnet-host}
    set replacemsg-override-group {string}
    set retransmission [disable|enable]
    set ring-rx {integer}
    set ring-tx {integer}
    set role [lan|wan|...]
    set sample-direction [tx|rx|...]
    set sample-rate {integer}
    set secondary-IP [enable|disable]
    config secondaryip

```

```

Description: Second IP address of interface.
edit <id>
    set allowaccess {option1}, {option2}, ...
    set detectprotocol {option1}, {option2}, ...
    set detectserver {user}
    set gwdetect [enable|disable]
    set ha-priority {integer}
    set ip {ipv4-classnet-host}
    set ping-serv-status {integer}
next
end
set security-8021x-dynamic-vlan-id {integer}
set security-8021x-master {string}
set security-8021x-mode [default|dynamic-vlan|...]
set security-exempt-list {string}
set security-external-logout {string}
set security-external-web {string}
set security-groups <name1>, <name2>, ...
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-mode [none|captive-portal|...]
set security-redirect-url {string}
set service-name {string}
set sflow-sampler [enable|disable]
set snmp-index {integer}
set speed [auto|10full|...]
set spillover-threshold {integer}
set src-check [enable|disable]
set status [up|down]
set stp [disable|enable]
set stp-ha-slave [disable|enable|...]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set subst [enable|disable]
set substitute-dst-mac {mac-address}
set switch {string}
set switch-controller-access-vlan [enable|disable]
set switch-controller-arp-inspection [enable|disable]
set switch-controller-dhcp-snooping [enable|disable]
set switch-controller-dhcp-snooping-option82 [enable|disable]
set switch-controller-dhcp-snooping-verify-mac [enable|disable]
set switch-controller-igmp-snooping [enable|disable]
set switch-controller-igmp-snooping-fast-leave [enable|disable]
set switch-controller-igmp-snooping-proxy [enable|disable]
set switch-controller-learning-limit {integer}
set switch-controller-rspan-mode [disable|enable]
set switch-controller-traffic-policy {string}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set tc-mode [ptm|atm]
set tcp-mss {integer}
set trunk [enable|disable]

```



```

set trust-ip-1 {ipv4-classnet-any}
set trust-ip-2 {ipv4-classnet-any}
set trust-ip-3 {ipv4-classnet-any}
set trust-ip6-1 {ipv6-prefix}
set trust-ip6-2 {ipv6-prefix}
set trust-ip6-3 {ipv6-prefix}
set type [physical|vlan|...]
set username {string}
set vci {integer}
set vdom {string}
set vectoring [disable|enable]
set vindex {integer}
set vlanforward [enable|disable]
set vlanid {integer}
set vpi {integer}
set vrf {integer}
config vrrp
    Description: VRRP configuration.
    edit <vrid>
        set accept-mode [enable|disable]
        set adv-interval {integer}
        set ignore-default-route [enable|disable]
        set preempt [enable|disable]
        set priority {integer}
        config proxy-arp
            Description: VRRP Proxy ARP configuration.
            edit <id>
                set ip {user}
            next
        end
        set start-time {integer}
        set status [enable|disable]
        set version [2|3]
        set vrdest {ipv4-address-any}
        set vrdest-priority {integer}
        set vrgrp {integer}
        set vrip {ipv4-address-any}
    next
end
set vrrp-virtual-mac [enable|disable]
set wccp [enable|disable]
set weight {integer}
set wifi-5g-threshold {string}
set wifi-acl [allow|deny]
set wifi-ap-band [any|5g-preferred|...]
set wifi-auth [PSK|radius|...]
set wifi-auto-connect [enable|disable]
set wifi-auto-save [enable|disable]
set wifi-broadcast-ssid [enable|disable]
set wifi-encrypt [TKIP|AES]
set wifi-fragment-threshold {integer}
set wifi-key {password}
set wifi-keyindex {integer}
set wifi-mac-filter [enable|disable]
config wifi-mac-list
    Description: MAC filter list.

```

```

        edit <id>
            set mac {mac-address}
        next
    end
    config wifi-networks
        Description: WiFi network table.
        edit <id>
            set wifi-encrypt [TKIP|AES]
            set wifi-key {password}
            set wifi-keyindex {integer}
            set wifi-passphrase {password}
            set wifi-security [open|wep64|...]
            set wifi-ssid {string}
        next
    end
    set wifi-passphrase {password}
    set wifi-radius-server {string}
    set wifi-rtt-threshold {integer}
    set wifi-security [open|wep64|...]
    set wifi-ssid {string}
    set wifi-usergroup {string}
    set wins-ip {ipv4-address}
next
end

```

config system interface

Parameter	Description	Type	Size								
ac-name	PPPoE server name.	string	Maximum length: 63								
aggregate *	Aggregate interface. Read-only.	string	Maximum length: 15								
algorithm *	Frame distribution algorithm.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>L2</td><td>Use layer 2 address for distribution.</td></tr><tr><td>L3</td><td>Use layer 3 address for distribution.</td></tr><tr><td>L4</td><td>Use layer 4 information for distribution.</td></tr></table>	Option	Description	L2	Use layer 2 address for distribution.	L3	Use layer 3 address for distribution.	L4	Use layer 4 information for distribution.		
Option	Description										
L2	Use layer 2 address for distribution.										
L3	Use layer 3 address for distribution.										
L4	Use layer 4 information for distribution.										
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25								
allowaccess	Permitted types of management access to this interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING access.</td></tr></table>	Option	Description	ping	PING access.						
Option	Description										
ping	PING access.										

Parameter	Description	Type	Size																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr><tr><td><i>probe-response</i></td><td>Probe access.</td></tr><tr><td><i>fabric</i></td><td>Security Fabric access.</td></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.		
	Option	Description																							
	<i>https</i>	HTTPS access.																							
	<i>ssh</i>	SSH access.																							
	<i>snmp</i>	SNMP access.																							
	<i>http</i>	HTTP access.																							
	<i>telnet</i>	TELNET access.																							
	<i>fgfm</i>	FortiManager access.																							
	<i>radius-acct</i>	RADIUS accounting access.																							
	<i>probe-response</i>	Probe access.																							
	<i>fabric</i>	Security Fabric access.																							
	<i>ftm</i>	FTM access.																							
ap-discover	Enable/disable automatic registration of unknown FortiAP devices.	option	-																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic registration of unknown FortiAP devices.</td></tr><tr><td><i>disable</i></td><td>Disable automatic registration of unknown FortiAP devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.	<i>disable</i>	Disable automatic registration of unknown FortiAP devices.																		
	Option	Description																							
	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.																							
<i>disable</i>	Disable automatic registration of unknown FortiAP devices.																								
arpforward	Enable/disable ARP forwarding.	option	-																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ARP forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable ARP forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable ARP forwarding.	<i>disable</i>	Disable ARP forwarding.																		
	Option	Description																							
	<i>enable</i>	Enable ARP forwarding.																							
<i>disable</i>	Disable ARP forwarding.																								
atm-protocol *	ATM protocol.	option	-																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Not over ATM.</td></tr><tr><td><i>ipoa</i></td><td>IPoA RFC2684.</td></tr></table>	Option	Description	<i>none</i>	Not over ATM.	<i>ipoa</i>	IPoA RFC2684.																		
	Option	Description																							
	<i>none</i>	Not over ATM.																							
<i>ipoa</i>	IPoA RFC2684.																								
auth-type	PPP authentication type to use.	option	-																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically choose authentication.</td></tr><tr><td><i>pap</i></td><td>PAP authentication.</td></tr></table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.																		
	Option	Description																							
	<i>auto</i>	Automatically choose authentication.																							
<i>pap</i>	PAP authentication.																								

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.		
	Option	Description									
	<i>chap</i>	CHAP authentication.									
	<i>mschapv1</i>	MS-CHAPv1 authentication.									
<i>mschapv2</i>	MS-CHAPv2 authentication.										
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension device on this interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic authorization of dedicated Fortinet extension device on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable automatic authorization of dedicated Fortinet extension device on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.				
	Option	Description									
	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.									
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.										
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>BFD behavior of this interface will be based on global configuration.</td></tr><tr><td><i>enable</i></td><td>Enable BFD on this interface and ignore global configuration.</td></tr><tr><td><i>disable</i></td><td>Disable BFD on this interface and ignore global configuration.</td></tr></table>	Option	Description	<i>global</i>	BFD behavior of this interface will be based on global configuration.	<i>enable</i>	Enable BFD on this interface and ignore global configuration.	<i>disable</i>	Disable BFD on this interface and ignore global configuration.		
	Option	Description									
	<i>global</i>	BFD behavior of this interface will be based on global configuration.									
	<i>enable</i>	Enable BFD on this interface and ignore global configuration.									
<i>disable</i>	Disable BFD on this interface and ignore global configuration.										
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000								
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								
broadcast-forticlient-discovery	Enable/disable broadcasting FortiClient discovery messages.	option	-								

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcasting FortiClient discovery messages.</td></tr><tr><td><i>disable</i></td><td>Disable broadcasting FortiClient discovery messages.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcasting FortiClient discovery messages.	<i>disable</i>	Disable broadcasting FortiClient discovery messages.		
	Option	Description							
	<i>enable</i>	Enable broadcasting FortiClient discovery messages.							
<i>disable</i>	Disable broadcasting FortiClient discovery messages.								
broadcast-forward	Enable/disable broadcast forwarding.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast forwarding.	<i>disable</i>	Disable broadcast forwarding.		
	Option	Description							
	<i>enable</i>	Enable broadcast forwarding.							
<i>disable</i>	Disable broadcast forwarding.								
cli-conn-status	CLI connection status. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295						
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32						
dedicated-to	Configure interface for single purpose.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Interface not dedicated for any purpose.</td></tr><tr><td><i>management</i></td><td>Dedicate this interface for management purposes only.</td></tr></table>	Option	Description	<i>none</i>	Interface not dedicated for any purpose.	<i>management</i>	Dedicate this interface for management purposes only.		
	Option	Description							
	<i>none</i>	Interface not dedicated for any purpose.							
<i>management</i>	Dedicate this interface for management purposes only.								
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable default gateway.</td></tr><tr><td><i>disable</i></td><td>Disable default gateway.</td></tr></table>	Option	Description	<i>enable</i>	Enable default gateway.	<i>disable</i>	Disable default gateway.		
	Option	Description							
	<i>enable</i>	Enable default gateway.							
<i>disable</i>	Disable default gateway.								
description	Description.	var-string	Maximum length: 255						
detected-peer-mtu	MTU of detected peer (0 - 4294967295). Read-only.	integer	Minimum value: 0 Maximum value: 4294967295						

Parameter	Description	Type	Size								
detectprotocol	Protocols used to detect the server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo.</td></tr></table>	Option	Description	<i>ping</i>	PING.	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.		
Option	Description										
<i>ping</i>	PING.										
<i>tcp-echo</i>	TCP echo.										
<i>udp-echo</i>	UDP echo.										
detectserver	Gateway's ping server for this IP.	user	Not Specified								
device-identification	Enable/disable passively gathering of device identity information about the devices on the network connected to this interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable passive gathering of identity information about hosts.</td></tr><tr><td><i>disable</i></td><td>Disable passive gathering of identity information about hosts.</td></tr></table>	Option	Description	<i>enable</i>	Enable passive gathering of identity information about hosts.	<i>disable</i>	Disable passive gathering of identity information about hosts.				
Option	Description										
<i>enable</i>	Enable passive gathering of identity information about hosts.										
<i>disable</i>	Disable passive gathering of identity information about hosts.										
device-user-identification	Enable/disable passive gathering of user identity information about users on this interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable passive gathering of user identity information about users.</td></tr><tr><td><i>disable</i></td><td>Disable passive gathering of user identity information about users.</td></tr></table>	Option	Description	<i>enable</i>	Enable passive gathering of user identity information about users.	<i>disable</i>	Disable passive gathering of user identity information about users.				
Option	Description										
<i>enable</i>	Enable passive gathering of user identity information about users.										
<i>disable</i>	Disable passive gathering of user identity information about users.										
devindex	Device Index. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295								
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48								
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP relay agent option.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP relay agent option.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP relay agent option.	<i>disable</i>	Disable DHCP relay agent option.				
Option	Description										
<i>enable</i>	Enable DHCP relay agent option.										
<i>disable</i>	Disable DHCP relay agent option.										
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15								

Parameter	Description	Type	Size								
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.		
Option	Description										
auto	Set outgoing interface automatically.										
sdwan	Set outgoing interface by SD-WAN or policy routing rules.										
specify	Set outgoing interface manually.										
dhcp-relay-ip	DHCP relay IP address.	user	Not Specified								
dhcp-relay-request-all-server	Enable/disable sending DHCP request to all servers.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only send DHCP request to matching server.</td></tr><tr><td>enable</td><td>Sending DHCP request to all servers.</td></tr></table>	Option	Description	disable	Only send DHCP request to matching server.	enable	Sending DHCP request to all servers.				
Option	Description										
disable	Only send DHCP request to matching server.										
enable	Sending DHCP request to all servers.										
dhcp-relay-service	Enable/disable allowing this interface to act as a DHCP relay.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>None.</td></tr><tr><td>enable</td><td>DHCP relay agent.</td></tr></table>	Option	Description	disable	None.	enable	DHCP relay agent.				
Option	Description										
disable	None.										
enable	DHCP relay agent.										
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>regular</td><td>Regular DHCP relay.</td></tr><tr><td>ipsec</td><td>DHCP relay for IPsec.</td></tr></table>	Option	Description	regular	Regular DHCP relay.	ipsec	DHCP relay for IPsec.				
Option	Description										
regular	Regular DHCP relay.										
ipsec	DHCP relay for IPsec.										
dhcp-renew-time	DHCP renew time in seconds (300-604800), 0 means use the renew time provided by the server.	integer	Minimum value: 300 Maximum value: 604800								
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								

Parameter	Description	Type	Size
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
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-

Option	Description
<i>enable</i>	Use DNS acquired by DHCP or PPPoE.
<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.

drop-fragment	Enable/disable drop fragment packets.	option	-

Option	Description
<i>enable</i>	Enable/disable drop fragment packets.
<i>disable</i>	Do not drop fragment packets.

drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-

Option	Description
<i>enable</i>	Enable drop of overlapped fragment packets.
<i>disable</i>	Disable drop of overlapped fragment packets.

egress-cos *	Override outgoing CoS in user VLAN tag.	option	-

Option	Description
<i>disable</i>	Disable.
<i>cos0</i>	CoS 0.
<i>cos1</i>	CoS 1.
<i>cos2</i>	CoS 2.
<i>cos3</i>	CoS 3.
<i>cos4</i>	CoS 4.
<i>cos5</i>	CoS 5.

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cos6</td><td>CoS 6.</td></tr><tr><td>cos7</td><td>CoS 7.</td></tr></table>	Option	Description	cos6	CoS 6.	cos7	CoS 7.		
	Option	Description							
	cos6	CoS 6.							
cos7	CoS 7.								
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35						
estimated-downstream-bandwidth	Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295						
estimated-upstream-bandwidth	Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295						
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable explicit FTP proxy on this interface.</td></tr><tr><td>disable</td><td>Disable explicit FTP proxy on this interface.</td></tr></table>	Option	Description	enable	Enable explicit FTP proxy on this interface.	disable	Disable explicit FTP proxy on this interface.		
	Option	Description							
	enable	Enable explicit FTP proxy on this interface.							
disable	Disable explicit FTP proxy on this interface.								
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable explicit Web proxy on this interface.</td></tr><tr><td>disable</td><td>Disable explicit Web proxy on this interface.</td></tr></table>	Option	Description	enable	Enable explicit Web proxy on this interface.	disable	Disable explicit Web proxy on this interface.		
	Option	Description							
	enable	Enable explicit Web proxy on this interface.							
disable	Disable explicit Web proxy on this interface.								
external	Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable identifying the interface as an external interface.</td></tr><tr><td>disable</td><td>Disable identifying the interface as an external interface.</td></tr></table>	Option	Description	enable	Enable identifying the interface as an external interface.	disable	Disable identifying the interface as an external interface.		
	Option	Description							
	enable	Enable identifying the interface as an external interface.							
disable	Disable identifying the interface as an external interface.								
fail-action-on-extender	Action on extender when interface fail .	option	-						

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>soft-restart</i></td><td>Soft-restart-on-extender.</td></tr><tr><td><i>hard-restart</i></td><td>Hard-restart-on-extender.</td></tr><tr><td><i>reboot</i></td><td>Reboot-on-extender.</td></tr></table>	Option	Description	<i>soft-restart</i>	Soft-restart-on-extender.	<i>hard-restart</i>	Hard-restart-on-extender.	<i>reboot</i>	Reboot-on-extender.		
	Option	Description									
	<i>soft-restart</i>	Soft-restart-on-extender.									
	<i>hard-restart</i>	Hard-restart-on-extender.									
<i>reboot</i>	Reboot-on-extender.										
fail-alert-interfaces <name>	Names of the FortiGate interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 79								
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>link-failed-signal</i></td><td>Link-failed-signal.</td></tr><tr><td><i>link-down</i></td><td>Link-down.</td></tr></table>	Option	Description	<i>link-failed-signal</i>	Link-failed-signal.	<i>link-down</i>	Link-down.				
	Option	Description									
	<i>link-failed-signal</i>	Link-failed-signal.									
<i>link-down</i>	Link-down.										
fail-detect	Enable/disable fail detection features for this interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable interface failed option status.</td></tr><tr><td><i>disable</i></td><td>Disable interface failed option status.</td></tr></table>	Option	Description	<i>enable</i>	Enable interface failed option status.	<i>disable</i>	Disable interface failed option status.				
	Option	Description									
	<i>enable</i>	Enable interface failed option status.									
<i>disable</i>	Disable interface failed option status.										
fail-detect-option	Options for detecting that this interface has failed.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>detectserver</i></td><td>Use a ping server to determine if the interface has failed.</td></tr><tr><td><i>link-down</i></td><td>Use port detection to determine if the interface has failed.</td></tr></table>	Option	Description	<i>detectserver</i>	Use a ping server to determine if the interface has failed.	<i>link-down</i>	Use port detection to determine if the interface has failed.				
	Option	Description									
	<i>detectserver</i>	Use a ping server to determine if the interface has failed.									
<i>link-down</i>	Use port detection to determine if the interface has failed.										
fortilink *	Enable FortiLink to dedicate this interface to manage other Fortinet devices.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink to dedicated interface for managing FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink to dedicated interface for managing FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.	<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.				
	Option	Description									
	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.									
<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.										
fortilink-backup-link	fortilink split interface backup link. Read-only.	integer	Minimum value: 0 Maximum value: 255								

Parameter	Description	Type	Size						
fortilink-neighbor-detect	Protocol for FortiGate neighbor discovery.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lldp</i></td><td>Detect FortiLink neighbors using LLDP protocol.</td></tr><tr><td><i>fortilink</i></td><td>Detect FortiLink neighbors using FortiLink protocol.</td></tr></table>	Option	Description	<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.	<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.		
Option	Description								
<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.								
<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.								
fortilink-split-interface	Enable/disable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink split interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	<i>disable</i>	Disable FortiLink split interface.		
Option	Description								
<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.								
<i>disable</i>	Disable FortiLink split interface.								
fortilink-stacking	Enable/disable FortiLink switch-stacking on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink switch stacking.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink switch stacking.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiLink switch stacking.	<i>disable</i>	Disable FortiLink switch stacking.		
Option	Description								
<i>enable</i>	Enable FortiLink switch stacking.								
<i>disable</i>	Disable FortiLink switch stacking.								
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 Maximum value: 2147483647						
forward-error-correction *	Enable/disable forward error correction (FEC Clause 91).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward error correction (FEC).</td></tr><tr><td><i>disable</i></td><td>Disable forward error correction (FEC).</td></tr></table>	Option	Description	<i>enable</i>	Enable forward error correction (FEC).	<i>disable</i>	Disable forward error correction (FEC).		
Option	Description								
<i>enable</i>	Enable forward error correction (FEC).								
<i>disable</i>	Disable forward error correction (FEC).								
gateway-address *	Gateway address	ipv4-address	Not Specified						
gwaddr *	Gateway address	ipv4-address	Not Specified						
gwdetect	Enable/disable detect gateway alive for first.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detect gateway alive for first.</td></tr><tr><td><i>disable</i></td><td>Disable detect gateway alive for first.</td></tr></table>	Option	Description	<i>enable</i>	Enable detect gateway alive for first.	<i>disable</i>	Disable detect gateway alive for first.		
	Option	Description							
	<i>enable</i>	Enable detect gateway alive for first.							
<i>disable</i>	Disable detect gateway alive for first.								
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50						
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICMP accept redirect.</td></tr><tr><td><i>disable</i></td><td>Disable ICMP accept redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICMP accept redirect.	<i>disable</i>	Disable ICMP accept redirect.		
	Option	Description							
	<i>enable</i>	Enable ICMP accept redirect.							
<i>disable</i>	Disable ICMP accept redirect.								
icmp-send-redirect	Enable/disable ICMP send redirect.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICMP send redirect.</td></tr><tr><td><i>disable</i></td><td>Disable ICMP send redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICMP send redirect.	<i>disable</i>	Disable ICMP send redirect.		
	Option	Description							
	<i>enable</i>	Enable ICMP send redirect.							
<i>disable</i>	Disable ICMP send redirect.								
ident-accept	Enable/disable authentication for this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable determining a user's identity from packet identification.</td></tr><tr><td><i>disable</i></td><td>Disable determining a user's identity from packet identification.</td></tr></table>	Option	Description	<i>enable</i>	Enable determining a user's identity from packet identification.	<i>disable</i>	Disable determining a user's identity from packet identification.		
	Option	Description							
	<i>enable</i>	Enable determining a user's identity from packet identification.							
<i>disable</i>	Disable determining a user's identity from packet identification.								
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 32767						
inbandwidth	Bandwidth limit for incoming traffic (0 - 16776000 kbps), 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000						
ingress-cos *	Override incoming CoS in user VLAN tag on VLAN interface or assign a priority VLAN tag on physical interface.	option	-						

Parameter	Description	Type	Size																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>cos0</i></td><td>CoS 0.</td></tr><tr><td><i>cos1</i></td><td>CoS 1.</td></tr><tr><td><i>cos2</i></td><td>CoS 2.</td></tr><tr><td><i>cos3</i></td><td>CoS 3.</td></tr><tr><td><i>cos4</i></td><td>CoS 4.</td></tr><tr><td><i>cos5</i></td><td>CoS 5.</td></tr><tr><td><i>cos6</i></td><td>CoS 6.</td></tr><tr><td><i>cos7</i></td><td>CoS 7.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>cos0</i>	CoS 0.	<i>cos1</i>	CoS 1.	<i>cos2</i>	CoS 2.	<i>cos3</i>	CoS 3.	<i>cos4</i>	CoS 4.	<i>cos5</i>	CoS 5.	<i>cos6</i>	CoS 6.	<i>cos7</i>	CoS 7.		
	Option	Description																					
	<i>disable</i>	Disable.																					
	<i>cos0</i>	CoS 0.																					
	<i>cos1</i>	CoS 1.																					
	<i>cos2</i>	CoS 2.																					
	<i>cos3</i>	CoS 3.																					
	<i>cos4</i>	CoS 4.																					
	<i>cos5</i>	CoS 5.																					
	<i>cos6</i>	CoS 6.																					
<i>cos7</i>	CoS 7.																						
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35																				
ingress-spillover-threshold	Ingress Spillover threshold (0 - 16776000 kbps).	integer	Minimum value: 0 Maximum value: 16776000																				
interface	Interface name.	string	Maximum length: 15																				
internal	Implicitly created.	integer	Minimum value: 0 Maximum value: 255																				
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified																				
ipmac	Enable/disable IP/MAC binding.	option	-																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP/MAC binding.</td></tr><tr><td><i>disable</i></td><td>Disable IP/MAC binding.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP/MAC binding.	<i>disable</i>	Disable IP/MAC binding.																
	Option	Description																					
	<i>enable</i>	Enable IP/MAC binding.																					
<i>disable</i>	Disable IP/MAC binding.																						
ips-sniffer-mode	Enable/disable the use of this interface as a one-armed sniffer.	option	-																				

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable IPS sniffer mode.	
	<i>disable</i>	Disable IPS sniffer mode.	
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified
l2forward	Enable/disable l2 forwarding.	option	-
	Option	Description	
	<i>enable</i>	Enable L2 forwarding.	
	<i>disable</i>	Disable L2 forwarding.	
l2tp-client *	Enable/disable this interface as a Layer 2 Tunneling Protocol (L2TP) client.	option	-
	Option	Description	
	<i>enable</i>	Enable L2TP client.	
	<i>disable</i>	Disable L2TP client.	
lACP-ha-slave *	LACP HA slave.	option	-
	Option	Description	
	<i>enable</i>	Allow HA slave to send/receive LACP messages.	
	<i>disable</i>	Block HA slave from sending/receiving LACP messages.	
lACP-mode *	LACP mode.	option	-
	Option	Description	
	<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.	
	<i>passive</i>	Passively use LACP to negotiate 802.3ad aggregation.	
	<i>active</i>	Actively use LACP to negotiate 802.3ad aggregation.	
lACP-speed *	How often the interface sends LACP messages.	option	-
	Option	Description	
	<i>slow</i>	Send LACP message every 30 seconds.	
	<i>fast</i>	Send LACP message every second.	

Parameter	Description	Type	Size
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
link-up-delay *	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000
lldp-network-policy	LLDP-MED network policy profile.	string	Maximum length: 35
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-

Option	Description
<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).
<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).
<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.

lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-

Option	Description
<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).
<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).
<i>vdom</i>	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.

macaddr	Change the interface's MAC address.	mac-address	Not Specified
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified
mediatype *	Select SFP media interface type	option	-

Option	Description
<i>serdes-sfp</i>	SFP using SerDes Media Interface

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sgmii-sfp</i></td><td>SFP using SGMII Media Interface</td></tr><tr><td><i>serdes-copper-sfp</i></td><td>Copper SFP using SerDes media Interface.</td></tr></table>	Option	Description	<i>sgmii-sfp</i>	SFP using SGMII Media Interface	<i>serdes-copper-sfp</i>	Copper SFP using SerDes media Interface.				
	Option	Description									
	<i>sgmii-sfp</i>	SFP using SGMII Media Interface									
<i>serdes-copper-sfp</i>	Copper SFP using SerDes media Interface.										
member <interface-name> *	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79								
min-links *	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32								
min-links-down *	Action to take when less than the configured minimum number of links are active.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>operational</i></td><td>Set the aggregate operationally down.</td></tr><tr><td><i>administrative</i></td><td>Set the aggregate administratively down.</td></tr></table>	Option	Description	<i>operational</i>	Set the aggregate operationally down.	<i>administrative</i>	Set the aggregate administratively down.				
	Option	Description									
	<i>operational</i>	Set the aggregate operationally down.									
<i>administrative</i>	Set the aggregate administratively down.										
mode	Addressing mode (static, DHCP, PPPoE).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static setting.</td></tr><tr><td><i>dhcp</i></td><td>External DHCP client mode.</td></tr><tr><td><i>pppoe</i></td><td>External PPPoE mode.</td></tr></table>	Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	External DHCP client mode.	<i>pppoe</i>	External PPPoE mode.		
	Option	Description									
	<i>static</i>	Static setting.									
	<i>dhcp</i>	External DHCP client mode.									
<i>pppoe</i>	External PPPoE mode.										
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295								
mtu-override	Enable to set a custom MTU for this interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override default MTU.</td></tr><tr><td><i>disable</i></td><td>Use default MTU (1500).</td></tr></table>	Option	Description	<i>enable</i>	Override default MTU.	<i>disable</i>	Use default MTU (1500).				
	Option	Description									
	<i>enable</i>	Override default MTU.									
<i>disable</i>	Use default MTU (1500).										
mux-type *	Multiplexer type	option	-								

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>llc-encaps</i></td><td>LLC encapsulation.</td></tr><tr><td><i>vc-encaps</i></td><td>VC encapsulation.</td></tr></table>	Option	Description	<i>llc-encaps</i>	LLC encapsulation.	<i>vc-encaps</i>	VC encapsulation.						
	Option	Description											
	<i>llc-encaps</i>	LLC encapsulation.											
<i>vc-encaps</i>	VC encapsulation.												
name	Name.	string	Maximum length: 15										
ndiscforward	Enable/disable NDISC forwarding.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NDISC forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable NDISC forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable NDISC forwarding.	<i>disable</i>	Disable NDISC forwarding.						
	Option	Description											
	<i>enable</i>	Enable NDISC forwarding.											
<i>disable</i>	Disable NDISC forwarding.												
netbios-forward	Enable/disable NETBIOS forwarding.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NETBIOS forwarding.</td></tr><tr><td><i>enable</i></td><td>Enable NETBIOS forwarding.</td></tr></table>	Option	Description	<i>disable</i>	Disable NETBIOS forwarding.	<i>enable</i>	Enable NETBIOS forwarding.						
	Option	Description											
	<i>disable</i>	Disable NETBIOS forwarding.											
<i>enable</i>	Enable NETBIOS forwarding.												
netflow-sampler	Enable/disable NetFlow on this interface and set the data that NetFlow collects (rx, tx, or both).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NetFlow protocol on this interface.</td></tr><tr><td><i>tx</i></td><td>Monitor transmitted traffic on this interface.</td></tr><tr><td><i>rx</i></td><td>Monitor received traffic on this interface.</td></tr><tr><td><i>both</i></td><td>Monitor transmitted/received traffic on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable NetFlow protocol on this interface.	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.		
	Option	Description											
	<i>disable</i>	Disable NetFlow protocol on this interface.											
	<i>tx</i>	Monitor transmitted traffic on this interface.											
	<i>rx</i>	Monitor received traffic on this interface.											
<i>both</i>	Monitor transmitted/received traffic on this interface.												
outbandwidth	Bandwidth limit for outgoing traffic (0 - 16776000 kbps).	integer	Minimum value: 0 Maximum value: 16776000										
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295										
password	PPPoE account's password.	password	Not Specified										
phy-mode *	DSL physical mode.	option	-										

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>adsl</i></td><td>ADSL/ADSL2/ADSL2+.</td></tr><tr><td><i>vdsl</i></td><td>VDSL.</td></tr></table>	Option	Description	<i>adsl</i>	ADSL/ADSL2/ADSL2+.	<i>vdsl</i>	VDSL.								
	Option	Description													
	<i>adsl</i>	ADSL/ADSL2/ADSL2+.													
<i>vdsl</i>	VDSL.														
ping-serv-status	PING server status. Read-only.	integer	Minimum value: 0 Maximum value: 255												
poe *	Enable/disable PoE status.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PoE status.</td></tr><tr><td><i>disable</i></td><td>Disable PoE status.</td></tr></table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.								
	Option	Description													
	<i>enable</i>	Enable PoE status.													
<i>disable</i>	Disable PoE status.														
polling-interval	sFlow polling interval (1 - 255 sec).	integer	Minimum value: 1 Maximum value: 255												
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP address negotiating for unnumbered.</td></tr><tr><td><i>disable</i></td><td>Disable IP address negotiating for unnumbered.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP address negotiating for unnumbered.	<i>disable</i>	Disable IP address negotiating for unnumbered.								
	Option	Description													
	<i>enable</i>	Enable IP address negotiating for unnumbered.													
<i>disable</i>	Disable IP address negotiating for unnumbered.														
pptp-auth-type	PPTP authentication type.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically choose authentication.</td></tr><tr><td><i>pap</i></td><td>PAP authentication.</td></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.		
	Option	Description													
	<i>auto</i>	Automatically choose authentication.													
	<i>pap</i>	PAP authentication.													
	<i>chap</i>	CHAP authentication.													
	<i>mschapv1</i>	MS-CHAPv1 authentication.													
<i>mschapv2</i>	MS-CHAPv2 authentication.														
pptp-client	Enable/disable PPTP client.	option	-												

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PPTP client.</td></tr><tr><td><i>disable</i></td><td>Disable PPTP client.</td></tr></table>	Option	Description	<i>enable</i>	Enable PPTP client.	<i>disable</i>	Disable PPTP client.		
	Option	Description							
	<i>enable</i>	Enable PPTP client.							
<i>disable</i>	Disable PPTP client.								
pptp-password	PPTP password.	password	Not Specified						
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified						
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535						
pptp-user	PPTP user name.	string	Maximum length: 64						
preserve-session-route	Enable/disable preservation of session route when dirty.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable preservation of session route when dirty.</td></tr><tr><td><i>disable</i></td><td>Disable preservation of session route when dirty.</td></tr></table>	Option	Description	<i>enable</i>	Enable preservation of session route when dirty.	<i>disable</i>	Disable preservation of session route when dirty.		
	Option	Description							
	<i>enable</i>	Enable preservation of session route when dirty.							
<i>disable</i>	Disable preservation of session route when dirty.								
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295						
priority-override *	Enable/disable fail back to higher priority port once recovered.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fail back to higher priority port once recovered.</td></tr><tr><td><i>disable</i></td><td>Disable fail back to higher priority port once recovered.</td></tr></table>	Option	Description	<i>enable</i>	Enable fail back to higher priority port once recovered.	<i>disable</i>	Disable fail back to higher priority port once recovered.		
	Option	Description							
	<i>enable</i>	Enable fail back to higher priority port once recovered.							
<i>disable</i>	Disable fail back to higher priority port once recovered.								
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable proxy captive portal on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable proxy captive portal on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable proxy captive portal on this interface.	<i>disable</i>	Disable proxy captive portal on this interface.		
	Option	Description							
	<i>enable</i>	Enable proxy captive portal on this interface.							
<i>disable</i>	Disable proxy captive portal on this interface.								
redundant-interface *	Redundant interface. Read-only.	string	Maximum length: 15						

Parameter	Description	Type	Size										
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified										
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35										
retransmission *	Enable/disable DSL retransmission.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable retransmission.</td></tr><tr><td><i>enable</i></td><td>Enable retransmission.</td></tr></table>			Option	Description	<i>disable</i>	Disable retransmission.	<i>enable</i>	Enable retransmission.				
	Option	Description											
	<i>disable</i>	Disable retransmission.											
<i>enable</i>	Enable retransmission.												
ring-rx *	RX ring size.	integer	Minimum value: 0 Maximum value: 4294967295										
ring-tx *	TX ring size.	integer	Minimum value: 0 Maximum value: 4294967295										
role	Interface role.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lan</i></td><td>Connected to local network of endpoints.</td></tr><tr><td><i>wan</i></td><td>Connected to Internet.</td></tr><tr><td><i>dmz</i></td><td>Connected to server zone.</td></tr><tr><td><i>undefined</i></td><td>Interface has no specific role.</td></tr></table>			Option	Description	<i>lan</i>	Connected to local network of endpoints.	<i>wan</i>	Connected to Internet.	<i>dmz</i>	Connected to server zone.	<i>undefined</i>	Interface has no specific role.
	Option	Description											
	<i>lan</i>	Connected to local network of endpoints.											
	<i>wan</i>	Connected to Internet.											
	<i>dmz</i>	Connected to server zone.											
<i>undefined</i>	Interface has no specific role.												
sample-direction	Data that NetFlow collects (rx, tx, or both).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tx</i></td><td>Monitor transmitted traffic on this interface.</td></tr><tr><td><i>rx</i></td><td>Monitor received traffic on this interface.</td></tr><tr><td><i>both</i></td><td>Monitor transmitted/received traffic on this interface.</td></tr></table>			Option	Description	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.		
	Option	Description											
	<i>tx</i>	Monitor transmitted traffic on this interface.											
	<i>rx</i>	Monitor received traffic on this interface.											
<i>both</i>	Monitor transmitted/received traffic on this interface.												
sample-rate	sFlow sample rate (10 - 99999).	integer	Minimum value: 10 Maximum value: 99999										

Parameter	Description	Type	Size
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-

Option	Description
<i>enable</i>	Enable secondary IP.
<i>disable</i>	Disable secondary IP.

security-8021x-dynamic-vlan-id *	VLAN ID for virtual switch.	integer	Minimum value: 0 Maximum value: 4094

security-8021x-master *	802.1X master virtual-switch.	string	Maximum length: 15

security-8021x-mode *	802.1X mode.	option	-

Option	Description
<i>default</i>	802.1X default mode.
<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.
<i>fallback</i>	802.1X fallback (master) mode.
<i>slave</i>	802.1X slave mode.

security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35

security-external-logout	URL of external authentication logout server.	string	Maximum length: 127

security-external-web	URL of external authentication web server.	string	Maximum length: 127

security-groups <name>	User groups that can authenticate with the captive portal. Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79

security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-

Option	Description
<i>mac-auth-only</i>	Enable MAC authentication bypass without EAP.
<i>enable</i>	Enable MAC authentication bypass.
<i>disable</i>	Disable MAC authentication bypass.

Parameter	Description	Type	Size
security-mode	Turn on captive portal authentication for this interface.	option	-

Option	Description
<i>none</i>	No security option.
<i>captive-portal</i>	Captive portal authentication.
<i>802.1X</i>	802.1X port-based authentication.

security-redirect-url	URL redirection after disclaimer/authentication.	string	Maximum length: 127
service-name	PPPoE service name.	string	Maximum length: 63
sflow-sampler	Enable/disable sFlow on this interface.	option	-

Option	Description
<i>enable</i>	Enable sFlow protocol on this interface.
<i>disable</i>	Disable sFlow protocol on this interface.

snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 0 Maximum value: 4294967295

speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-

Option	Description
<i>auto</i>	Automatically adjust speed.
<i>10full</i>	10M full-duplex.
<i>10half</i>	10M half-duplex.
<i>100full</i>	100M full-duplex.
<i>100half</i>	100M half-duplex.
<i>1000full</i>	1000M full-duplex.
<i>1000half</i>	1000M half-duplex.
<i>1000auto</i>	1000M auto adjust.
<i>10000full</i>	10G full-duplex.

Parameter	Description	Type	Size								
spillover-threshold	Egress Spillover threshold (0 - 16776000 kbps), 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000								
src-check	Enable/disable source IP check.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source IP check.</td></tr><tr><td><i>disable</i></td><td>Disable source IP check.</td></tr></table>	Option	Description	<i>enable</i>	Enable source IP check.	<i>disable</i>	Disable source IP check.				
Option	Description										
<i>enable</i>	Enable source IP check.										
<i>disable</i>	Disable source IP check.										
status	Bring the interface up or shut the interface down.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>up</i></td><td>Bring the interface up.</td></tr><tr><td><i>down</i></td><td>Shut the interface down.</td></tr></table>	Option	Description	<i>up</i>	Bring the interface up.	<i>down</i>	Shut the interface down.				
Option	Description										
<i>up</i>	Bring the interface up.										
<i>down</i>	Shut the interface down.										
stp *	Enable/disable STP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP.</td></tr><tr><td><i>enable</i></td><td>Enable STP.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP.	<i>enable</i>	Enable STP.				
Option	Description										
<i>disable</i>	Disable STP.										
<i>enable</i>	Enable STP.										
stp-ha-slave *	Control STP behaviour on HA slave.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP negotiation on HA slave.</td></tr><tr><td><i>enable</i></td><td>Enable STP negotiation on HA slave.</td></tr><tr><td><i>priority-adjust</i></td><td>Enable STP negotiation on HA slave and make priority lower than master.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP negotiation on HA slave.	<i>enable</i>	Enable STP negotiation on HA slave.	<i>priority-adjust</i>	Enable STP negotiation on HA slave and make priority lower than master.		
Option	Description										
<i>disable</i>	Disable STP negotiation on HA slave.										
<i>enable</i>	Enable STP negotiation on HA slave.										
<i>priority-adjust</i>	Enable STP negotiation on HA slave and make priority lower than master.										
stpforward	Enable/disable STP forwarding.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable STP forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable STP forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable STP forwarding.	<i>disable</i>	Disable STP forwarding.				
Option	Description										
<i>enable</i>	Enable STP forwarding.										
<i>disable</i>	Disable STP forwarding.										
stpforward-mode	Configure STP forwarding mode.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).	
	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.	
	<i>rpl-nothing</i>	Replace nothing.	
subst	Enable to always send packets from this interface to a destination MAC address.	option	-
	Option	Description	
	<i>enable</i>	Send packets from this interface.	
	<i>disable</i>	Do not send packets from this interface.	
substitute-dst-mac	Destination MAC address that all packets are sent to from this interface.	mac-address	Not Specified
switch	Contained in switch. Read-only.	string	Maximum length: 15
switch-controller-access-vlan *	Block FortiSwitch port-to-port traffic.	option	-
	Option	Description	
	<i>enable</i>	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.	
	<i>disable</i>	Allow normal VLAN traffic.	
switch-controller-arp-inspection *	Enable/disable FortiSwitch ARP inspection.	option	-
	Option	Description	
	<i>enable</i>	Enable ARP inspection for FortiSwitch devices.	
	<i>disable</i>	Disable ARP inspection for FortiSwitch devices.	
switch-controller-dhcp-snooping *	Switch controller DHCP snooping.	option	-
	Option	Description	
	<i>enable</i>	Enable DHCP snooping for FortiSwitch devices.	
	<i>disable</i>	Disable DHCP snooping for FortiSwitch devices.	

Parameter	Description	Type	Size						
switch-controller-dhcp-snooping-option82 *	Switch controller DHCP snooping option82.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP snooping insert option82 for FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP snooping insert option82 for FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.		
Option	Description								
<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.								
<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.								
switch-controller-dhcp-snooping-verify-mac *	Switch controller DHCP snooping verify MAC.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP snooping verify source MAC for FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP snooping verify source MAC for FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.		
Option	Description								
<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.								
<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.								
switch-controller-igmp-snooping *	Switch controller IGMP snooping.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP snooping.	<i>disable</i>	Disable IGMP snooping.		
Option	Description								
<i>enable</i>	Enable IGMP snooping.								
<i>disable</i>	Disable IGMP snooping.								
switch-controller-igmp-snooping-fast-leave *	Switch controller IGMP snooping fast-leave.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping fast-leave.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping fast-leave.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP snooping fast-leave.	<i>disable</i>	Disable IGMP snooping fast-leave.		
Option	Description								
<i>enable</i>	Enable IGMP snooping fast-leave.								
<i>disable</i>	Disable IGMP snooping fast-leave.								
switch-controller-igmp-snooping-proxy *	Switch controller IGMP snooping proxy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping proxy.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP snooping proxy.	<i>disable</i>	Disable IGMP snooping proxy.		
Option	Description								
<i>enable</i>	Enable IGMP snooping proxy.								
<i>disable</i>	Disable IGMP snooping proxy.								

Parameter	Description	Type	Size						
switch-controller-learning-limit *	Limit the number of dynamic MAC addresses on this VLAN (1 - 128, 0 = no limit, default).	integer	Minimum value: 0 Maximum value: 128						
switch-controller-rspan-mode *	Stop Layer2 MAC learning and interception of BPDUs and other packets on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable RSPAN passthrough mode on this VLAN interface.</td></tr><tr><td><i>enable</i></td><td>Enable RSPAN passthrough mode on this VLAN interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable RSPAN passthrough mode on this VLAN interface.	<i>enable</i>	Enable RSPAN passthrough mode on this VLAN interface.		
Option	Description								
<i>disable</i>	Disable RSPAN passthrough mode on this VLAN interface.								
<i>enable</i>	Enable RSPAN passthrough mode on this VLAN interface.								
switch-controller-traffic-policy *	Switch controller traffic policy for the VLAN.	string	Maximum length: 63						
tc-mode *	DSL transfer mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ptm</i></td><td>Packet transfer mode.</td></tr><tr><td><i>atm</i></td><td>Asynchronous transfer mode.</td></tr></table>	Option	Description	<i>ptm</i>	Packet transfer mode.	<i>atm</i>	Asynchronous transfer mode.		
Option	Description								
<i>ptm</i>	Packet transfer mode.								
<i>atm</i>	Asynchronous transfer mode.								
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 0 Maximum value: 4294967295						
trunk *	Enable/disable VLAN trunk.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VLAN trunk on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable VLAN trunk on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable VLAN trunk on this interface.	<i>disable</i>	Disable VLAN trunk on this interface.		
Option	Description								
<i>enable</i>	Enable VLAN trunk on this interface.								
<i>disable</i>	Disable VLAN trunk on this interface.								
trust-ip-1	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified						
trust-ip-2	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified						
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						

Parameter	Description	Type	Size
trust-ip6-3	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified
type	Interface type.	option	-

Option	Description
<i>physical</i>	Physical interface.
<i>vlan</i>	VLAN interface.
<i>aggregate</i>	Aggregate interface.
<i>redundant</i>	Redundant interface.
<i>tunnel</i>	Tunnel interface.
<i>vdom-link</i>	VDOM link interface.
<i>loopback</i>	Loopback interface.
<i>switch</i>	Software switch interface.
<i>vap-switch</i>	VAP interface.
<i>wl-mesh</i>	WLAN mesh interface.
<i>fext-wan</i>	FortiExtender interface.
<i>vxlan</i>	VXLAN interface.
<i>geneve</i>	GENEVE interface.
<i>hdlc</i>	T1/E1 interface.
<i>switch-vlan</i>	Switch VLAN interface.
<i>emac-vlan</i>	EMAC VLAN interface.

username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64
vci *	Virtual Channel ID	integer	Minimum value: 0 Maximum value: 65535
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31
vectoring *	Enable/disable DSL vectoring.	option	-

Option	Description
<i>disable</i>	Disable vectoring.
<i>enable</i>	Enable vectoring.

Parameter	Description	Type	Size						
vindex *	Switch control interface VLAN ID. Read-only.	integer	Minimum value: 0 Maximum value: 65535						
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable traffic forwarding.</td></tr><tr><td>disable</td><td>Disable traffic forwarding.</td></tr></table>	Option	Description	enable	Enable traffic forwarding.	disable	Disable traffic forwarding.		
Option	Description								
enable	Enable traffic forwarding.								
disable	Disable traffic forwarding.								
vlanid	VLAN ID (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094						
vpi *	Virtual Path ID	integer	Minimum value: 0 Maximum value: 255						
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31						
vrrp-virtual-mac	Enable/disable use of virtual MAC for VRRP.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of virtual MAC for VRRP.</td></tr><tr><td>disable</td><td>Disable use of virtual MAC for VRRP.</td></tr></table>	Option	Description	enable	Enable use of virtual MAC for VRRP.	disable	Disable use of virtual MAC for VRRP.		
Option	Description								
enable	Enable use of virtual MAC for VRRP.								
disable	Disable use of virtual MAC for VRRP.								
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WCCP protocol on this interface.</td></tr><tr><td>disable</td><td>Disable WCCP protocol on this interface.</td></tr></table>	Option	Description	enable	Enable WCCP protocol on this interface.	disable	Disable WCCP protocol on this interface.		
Option	Description								
enable	Enable WCCP protocol on this interface.								
disable	Disable WCCP protocol on this interface.								
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255						

Parameter	Description	Type	Size								
wifi-5g-threshold *	Minimal signal strength to be considered as a good 5G AP.	string	Maximum length: 7								
wifi-acl *	Access control for MAC addresses in the MAC list.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>	Option	Description	<i>allow</i>	Allow.	<i>deny</i>	Deny.				
Option	Description										
<i>allow</i>	Allow.										
<i>deny</i>	Deny.										
wifi-ap-band *	How to select the AP to connect.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Connect to the best 2G or 5G AP.</td></tr><tr><td><i>5g-preferred</i></td><td>Connect to the 5G AP if a good 5G AP exists.</td></tr><tr><td><i>5g-only</i></td><td>Only connect to the 5G AP.</td></tr></table>	Option	Description	<i>any</i>	Connect to the best 2G or 5G AP.	<i>5g-preferred</i>	Connect to the 5G AP if a good 5G AP exists.	<i>5g-only</i>	Only connect to the 5G AP.		
Option	Description										
<i>any</i>	Connect to the best 2G or 5G AP.										
<i>5g-preferred</i>	Connect to the 5G AP if a good 5G AP exists.										
<i>5g-only</i>	Only connect to the 5G AP.										
wifi-auth *	WiFi authentication.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>PSK</i></td><td>PSK.</td></tr><tr><td><i>radius</i></td><td>RADIUS.</td></tr><tr><td><i>usergroup</i></td><td>User group.</td></tr></table>	Option	Description	<i>PSK</i>	PSK.	<i>radius</i>	RADIUS.	<i>usergroup</i>	User group.		
Option	Description										
<i>PSK</i>	PSK.										
<i>radius</i>	RADIUS.										
<i>usergroup</i>	User group.										
wifi-auto-connect *	Enable/disable WiFi network auto connect.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi network auto connect.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi network auto connect.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi network auto connect.	<i>disable</i>	Disable WiFi network auto connect.				
Option	Description										
<i>enable</i>	Enable WiFi network auto connect.										
<i>disable</i>	Disable WiFi network auto connect.										
wifi-auto-save *	Enable/disable WiFi network automatic save.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi network automatic save.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi network automatic save.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi network automatic save.	<i>disable</i>	Disable WiFi network automatic save.				
Option	Description										
<i>enable</i>	Enable WiFi network automatic save.										
<i>disable</i>	Disable WiFi network automatic save.										
wifi-broadcast-ssid *	Enable/disable SSID broadcast in the beacon.	option	-								

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSID broadcast in the beacon.</td></tr><tr><td><i>disable</i></td><td>Disable SSID broadcast in the beacon.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSID broadcast in the beacon.	<i>disable</i>	Disable SSID broadcast in the beacon.				
	Option	Description									
	<i>enable</i>	Enable SSID broadcast in the beacon.									
<i>disable</i>	Disable SSID broadcast in the beacon.										
wifi-encrypt *	Data encryption.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TKIP</i></td><td>TKIP.</td></tr><tr><td><i>AES</i></td><td>AES.</td></tr></table>	Option	Description	<i>TKIP</i>	TKIP.	<i>AES</i>	AES.				
	Option	Description									
	<i>TKIP</i>	TKIP.									
<i>AES</i>	AES.										
wifi-fragment-threshold *	WiFi fragment threshold (800 - 2346).	integer	Minimum value: 800 Maximum value: 2346								
wifi-key *	WiFi WEP Key.	password	Not Specified								
wifi-keyindex *	WEP key index (1 - 4).	integer	Minimum value: 1 Maximum value: 4								
wifi-mac-filter *	Enable/disable MAC filter status.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC filter.</td></tr><tr><td><i>disable</i></td><td>Disable MAC filter.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC filter.	<i>disable</i>	Disable MAC filter.				
	Option	Description									
	<i>enable</i>	Enable MAC filter.									
<i>disable</i>	Disable MAC filter.										
wifi-passphrase *	WiFi pre-shared key for WPA.	password	Not Specified								
wifi-radius-server *	WiFi RADIUS server for WPA.	string	Maximum length: 35								
wifi-rts-threshold *	WiFi RTS threshold (256 - 2346).	integer	Minimum value: 256 Maximum value: 2346								
wifi-security *	Wireless access security of SSID.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wep64</i></td><td>WEP64.</td></tr><tr><td><i>wep128</i></td><td>WEP128.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wep64</i>	WEP64.	<i>wep128</i>	WEP128.		
	Option	Description									
	<i>open</i>	Open.									
	<i>wep64</i>	WEP64.									
<i>wep128</i>	WEP128.										

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wpa-personal</i></td><td>WPA personal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA enterprise.</td></tr><tr><td><i>wpa-only-personal</i></td><td>WPA personal only.</td></tr><tr><td><i>wpa-only-enterprise</i></td><td>WPA enterprise only.</td></tr><tr><td><i>wpa2-only-personal</i></td><td>WPA2 personal only.</td></tr><tr><td><i>wpa2-only-enterprise</i></td><td>WPA2 enterprise only.</td></tr></table>	Option	Description	<i>wpa-personal</i>	WPA personal.	<i>wpa-enterprise</i>	WPA enterprise.	<i>wpa-only-personal</i>	WPA personal only.	<i>wpa-only-enterprise</i>	WPA enterprise only.	<i>wpa2-only-personal</i>	WPA2 personal only.	<i>wpa2-only-enterprise</i>	WPA2 enterprise only.		
	Option	Description															
	<i>wpa-personal</i>	WPA personal.															
	<i>wpa-enterprise</i>	WPA enterprise.															
	<i>wpa-only-personal</i>	WPA personal only.															
	<i>wpa-only-enterprise</i>	WPA enterprise only.															
	<i>wpa2-only-personal</i>	WPA2 personal only.															
<i>wpa2-only-enterprise</i>	WPA2 enterprise only.																
wifi-ssid *	IEEE 802.11 Service Set Identifier.	string	Maximum length: 32														
wifi-usergroup *	WiFi user group for WPA.	string	Maximum length: 35														
wins-ip	WINS server IP.	ipv4-address	Not Specified														

* This parameter may not exist in some models.

config egress-queues

Parameter	Description	Type	Size
cos0	CoS profile name for CoS 0.	string	Maximum length: 35
cos1	CoS profile name for CoS 1.	string	Maximum length: 35
cos2	CoS profile name for CoS 2.	string	Maximum length: 35
cos3	CoS profile name for CoS 3.	string	Maximum length: 35
cos4	CoS profile name for CoS 4.	string	Maximum length: 35
cos5	CoS profile name for CoS 5.	string	Maximum length: 35
cos6	CoS profile name for CoS 6.	string	Maximum length: 35
cos7	CoS profile name for CoS 7.	string	Maximum length: 35

config ipv6

Parameter	Description	Type	Size
autoconf	Enable/disable address auto config.	option	-
	Option	Description	
	<i>enable</i>	Enable auto-configuration.	
	<i>disable</i>	Disable auto-configuration.	
dhcp6-client-options	DHCPv6 client options. Read-only.	option	-
	Option	Description	
	<i>rapid</i>	Send rapid commit option.	
	<i>iapd</i>	Send including IA-PD option.	
	<i>iana</i>	Send including IA-NA option.	
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-
	Option	Description	
	<i>enable</i>	Enable DHCPv6 information request.	
	<i>disable</i>	Disable DHCPv6 information request.	
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-
	Option	Description	
	<i>enable</i>	Enable DHCPv6 prefix delegation.	
	<i>disable</i>	Disable DHCPv6 prefix delegation.	
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

Parameter	Description	Type	Size
dhcp6-prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-

Option	Description
<i>disable</i>	Disable DHCPv6 relay
<i>enable</i>	Enable DHCPv6 relay.

dhcp6-relay-type	DHCPv6 relay type.	option	-

Option	Description
<i>regular</i>	Regular DHCP relay.

ip6-address	Primary IPv6 address prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx	ipv6-prefix	Not Specified
ip6-allowaccess	Allow management access to the interface.	option	-

Option	Description
<i>ping</i>	PING access.
<i>https</i>	HTTPS access.
<i>ssh</i>	SSH access.
<i>snmp</i>	SNMP access.
<i>http</i>	HTTP access.
<i>telnet</i>	TELNET access.
<i>fgfm</i>	FortiManager access.
<i>fabric</i>	Fabric access.

ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000

Parameter	Description	Type	Size
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-
	Option	Description	
	<i>enable</i>	Enable using the DNS server acquired by DHCP.	
	<i>disable</i>	Disable using the DNS server acquired by DHCP.	
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000
ip6-manage-flag	Enable/disable the managed flag.	option	-
	Option	Description	
	<i>enable</i>	Enable the managed IPv6 flag.	
	<i>disable</i>	Disable the managed IPv6 flag.	
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-
	Option	Description	
	<i>static</i>	Static setting.	
	<i>dhcp</i>	DHCPv6 client mode.	
	<i>pppoe</i>	IPv6 over PPPoE mode.	
	<i>delegated</i>	IPv6 address with delegated prefix.	
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable the other IPv6 flag.
<i>disable</i>	Disable the other IPv6 flag.

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-send-adv	Enable/disable sending advertisements about the interface.	option	-

Option	Description
<i>enable</i>	Enable sending advertisements about this interface.
<i>disable</i>	Disable sending advertisements about this interface.

ip6-subnet	Subnet to routing prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx	ipv6-prefix	Not Specified
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified
nd-mode	Neighbor discovery mode.	option	-

Option	Description
<i>basic</i>	Do not support SEND.
<i>SEND-compatible</i>	Support SEND.

nd-security-level	Neighbor discovery security level (0 - 7; 0 = least secure, default = 0).	integer	Minimum value: 0 Maximum value: 7

Parameter	Description	Type	Size
nd-timestamp-delta	Neighbor discovery timestamp delta value (1 - 3600 sec; default = 300).	integer	Minimum value: 1 Maximum value: 3600
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor (1 - 60 sec; default = 1).	integer	Minimum value: 1 Maximum value: 60
vrp6_link_local	Link-local IPv6 address of virtual router.	ipv6-address	Not Specified
vrrp-virtual-mac6	Enable/disable virtual MAC for VRRP.	option	-

Option	Description

<i>enable</i>	Enable virtual MAC for VRRP.
<i>disable</i>	Disable virtual MAC for VRRP.

config ip6-delegated-prefix-list

Parameter	Description	Type	Size
autonomous-flag	Enable/disable the autonomous flag.	option	-
	Option	Description	
	<i>enable</i>	Enable the autonomous flag.	
	<i>disable</i>	Disable the autonomous flag.	
onlink-flag	Enable/disable the onlink flag.	option	-
	Option	Description	
	<i>enable</i>	Enable the onlink flag.	
	<i>disable</i>	Disable the onlink flag.	
prefix-id	Prefix ID.	integer	Minimum value: 0 Maximum value: 4294967295
rdnss	Recursive DNS server option.	user	Not Specified
rdnss-service	Recursive DNS service option.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>delegated</i>	Delegated RDNSS settings.	
	<i>default</i>	System RDNSS settings.	
	<i>specify</i>	Specify recursive DNS servers.	
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15

config ip6-extra-addr

Parameter	Description	Type	Size
prefix	IPv6 address prefix.	ipv6-prefix	Not Specified

config ip6-prefix-list

Parameter	Description	Type	Size						
autonomous-flag	Enable/disable the autonomous flag.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the autonomous flag.</td></tr><tr><td><i>disable</i></td><td>Disable the autonomous flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the autonomous flag.	<i>disable</i>	Disable the autonomous flag.		
Option	Description								
<i>enable</i>	Enable the autonomous flag.								
<i>disable</i>	Disable the autonomous flag.								
dnssl <domain>	DNS search list option. Domain name.	string	Maximum length: 79						
onlink-flag	Enable/disable the onlink flag.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the onlink flag.</td></tr><tr><td><i>disable</i></td><td>Disable the onlink flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the onlink flag.	<i>disable</i>	Disable the onlink flag.		
Option	Description								
<i>enable</i>	Enable the onlink flag.								
<i>disable</i>	Disable the onlink flag.								
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295						
prefix	IPv6 prefix.	ipv6-network	Not Specified						
rdnss	Recursive DNS server option.	user	Not Specified						

Parameter	Description	Type	Size
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295

config vrrp6

Parameter	Description	Type	Size
accept-mode	Enable/disable accept mode.	option	-
	Option	Description	
	<i>enable</i>	Enable accept mode.	
	<i>disable</i>	Disable accept mode.	
adv-interval	Advertisement interval (1 - 255 seconds).	integer	Minimum value: 1 Maximum value: 255
preempt	Enable/disable preempt mode.	option	-
	Option	Description	
	<i>enable</i>	Enable preempt mode.	
	<i>disable</i>	Disable preempt mode.	
priority	Priority of the virtual router (1 - 255).	integer	Minimum value: 1 Maximum value: 255
start-time	Startup time (1 - 255 seconds).	integer	Minimum value: 1 Maximum value: 255
status	Enable/disable VRRP.	option	-
	Option	Description	
	<i>enable</i>	Enable VRRP.	
	<i>disable</i>	Disable VRRP.	
vrdst6	Monitor the route to this destination.	ipv6-address	Not Specified

Parameter	Description	Type	Size
vrrp	VRRP group ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535
vrid	Virtual router identifier (1 - 255).	integer	Minimum value: 1 Maximum value: 255
vrp6	IPv6 address of the virtual router.	ipv6-address	Not Specified

config l2tp-client-settings

Parameter	Description	Type	Size
auth-type	L2TP authentication type.	option	-
	Option	Description	
	<i>auto</i>	Automatically choose authentication.	
	<i>pap</i>	PAP authentication.	
	<i>chap</i>	CHAP authentication.	
	<i>mschapv1</i>	MS-CHAPv1 authentication.	
	<i>mschapv2</i>	MS-CHAPv2 authentication.	
defaultgw	Enable/disable default gateway.	option	-
	Option	Description	
	<i>enable</i>	Enable default gateway.	
	<i>disable</i>	Disable default gateway.	
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255
ip	IP. Read-only.	ipv4-classnet-host	Not Specified
mtu	L2TP MTU.	integer	Minimum value: 40 Maximum value: 65535
password	L2TP password.	password	Not Specified

Parameter	Description	Type	Size
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
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295
user	L2TP user name.	string	Maximum length: 127

config secondaryip

Parameter	Description	Type	Size
allowaccess	Management access settings for the secondary IP address.	option	-

Option	Description
<i>ping</i>	PING access.
<i>https</i>	HTTPS access.
<i>ssh</i>	SSH access.
<i>snmp</i>	SNMP access.
<i>http</i>	HTTP access.
<i>telnet</i>	TELNET access.
<i>fgfm</i>	FortiManager access.
<i>radius-acct</i>	RADIUS accounting access.
<i>probe-response</i>	Probe access.
<i>fabric</i>	Security Fabric access.
<i>ftm</i>	FTM access.

detectprotocol	Protocols used to detect the server.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>ping</i>	PING.	
	<i>tcp-echo</i>	TCP echo.	
	<i>udp-echo</i>	UDP echo.	
detectserver	Gateway's ping server for this IP.	user	Not Specified
gwdetect	Enable/disable detect gateway alive for first.	option	-
	Option	Description	
	<i>enable</i>	Enable detect gateway alive for first.	
	<i>disable</i>	Disable detect gateway alive for first.	
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified
ping-serv-status	PING server status. Read-only.	integer	Minimum value: 0 Maximum value: 255

config tagging

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

config vrrp

Parameter	Description	Type	Size
accept-mode	Enable/disable accept mode.	option	-
	Option Description		
	<i>enable</i>	Enable accept mode.	
	<i>disable</i>	Disable accept mode.	
adv-interval	Advertisement interval (1 - 255 seconds).	integer	Minimum value: 1 Maximum value: 255
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-
	Option Description		
	<i>enable</i>	Enable ignoring of default route when checking destination.	
	<i>disable</i>	Disable ignoring of default route when checking destination.	
preempt	Enable/disable preempt mode.	option	-
	Option Description		
	<i>enable</i>	Enable preempt mode.	
	<i>disable</i>	Disable preempt mode.	
priority	Priority of the virtual router (1 - 255).	integer	Minimum value: 1 Maximum value: 255
start-time	Startup time (1 - 255 seconds).	integer	Minimum value: 1 Maximum value: 255
status	Enable/disable this VRRP configuration.	option	-
	Option Description		
	<i>enable</i>	Enable this VRRP configuration.	
	<i>disable</i>	Disable this VRRP configuration.	
version	VRRP version.	option	-

Parameter	Description	Type	Size
	Option	Description	
	2	VRRP version 2.	
	3	VRRP version 3.	
vrdst	Monitor the route to this destination.	ipv4-address-any	Not Specified
vrdst-priority	Priority of the virtual router when the virtual router destination becomes unreachable (0 - 254).	integer	Minimum value: 0 Maximum value: 254
vrgrp	VRRP group ID (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535
vrid	Virtual router identifier (1 - 255).	integer	Minimum value: 1 Maximum value: 255
vrp	IP address of the virtual router.	ipv4-address-any	Not Specified

config proxy-arp

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	Set IP addresses of proxy ARP.	user	Not Specified

config wifi-mac-list

Parameter	Description	Type	Size
id	Id	integer	Minimum value: 0 Maximum value: 4294967295
mac	MAC address.	mac-address	Not Specified

config wifi-networks

Parameter	Description	Type	Size
id	Id	integer	Minimum value: 0 Maximum value: 4294967295
wifi-encrypt	Data encryption.	option	-
	Option	Description	
	TKIP	TKIP.	
	AES	AES.	
wifi-key	WiFi WEP Key.	password	Not Specified
wifi-keyindex	WEP key index (1 - 4).	integer	Minimum value: 1 Maximum value: 4
wifi-passphrase	WiFi pre-shared key for WPA.	password	Not Specified
wifi-security	Wireless access security of SSID.	option	-
	Option	Description	
	open	Open.	
	wep64	WEP64.	
	wep128	WEP128.	
	wpa-personal	WPA personal.	
	wpa-only-personal	WPA personal only.	
	wpa2-only-personal	WPA2 personal only.	
wifi-ssid	IEEE 802.11 Service Set Identifier.	string	Maximum length: 32

config system ipip-tunnel

Configure IP in IP Tunneling.

```
config system ipip-tunnel
    Description: Configure IP in IP Tunneling.
```

```

edit <name>
    set auto-asic-offload [enable|disable]
    set interface {string}
    set local-gw {ipv4-address-any}
    set remote-gw {ipv4-address}
next
end

```

config system ipip-tunnel

Parameter	Description	Type	Size
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-
	Option	Description	
	<i>enable</i>	Enable auto ASIC offloading.	
	<i>disable</i>	Disable ASIC offloading.	
interface	Interface name that is associated with the incoming traffic from available options.	string	Maximum length: 15
local-gw	IPv4 address for the local gateway.	ipv4-address-any	Not Specified
name	IPIP Tunnel name.	string	Maximum length: 15
remote-gw	IPv4 address for the remote gateway.	ipv4-address	Not Specified

* This parameter may not exist in some models.

config system ipsec-aggregate

Configure an aggregate of IPsec tunnels.

```

config system ipsec-aggregate
    Description: Configure an aggregate of IPsec tunnels.
    edit <name>
        set algorithm [L3|L4|...]
        set member <tunnel-name1>, <tunnel-name2>, ...
    next
end

```

config system ipsec-aggregate

Parameter	Description	Type	Size										
algorithm	Frame distribution algorithm.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>L3</td><td>Use layer 3 address for distribution.</td></tr><tr><td>L4</td><td>Use layer 4 information for distribution.</td></tr><tr><td>round-robin</td><td>Per-packet round-robin distribution.</td></tr><tr><td>redundant</td><td>Use first tunnel that is up for all traffic.</td></tr></table>	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.		
	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.												
member <tunnel-name>	Member tunnels of the aggregate. Tunnel name.	string	Maximum length: 79										
name	IPsec aggregate name.	string	Maximum length: 15										

config system ips-urlfilter-dns

Configure IPS URL filter DNS servers.

```
config system ips-urlfilter-dns
  Description: Configure IPS URL filter DNS servers.
  edit <address>
    set ipv6-capability [enable|disable]
    set status [enable|disable]
  next
end
```

config system ips-urlfilter-dns

Parameter	Description	Type	Size
address	DNS server IP address.	ipv4-address	Not Specified
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable this DNS server for IPS URL filter DNS queries.	
	<i>disable</i>	Disable this DNS server for IPS URL filter DNS queries.	

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
address6	IPv6 address of DNS server.	ipv6-address	Not Specified
status	Enable/disable this server for IPv6 DNS queries.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config system ipv6-neighbor-cache

Configure IPv6 neighbor cache table.

```
config system ipv6-neighbor-cache
    Description: Configure IPv6 neighbor cache table.
    edit <id>
        set interface {string}
        set ipv6 {ipv6-address}
        set mac {mac-address}
    next
end
```

config system ipv6-neighbor-cache

Parameter	Description	Type	Size
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295
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 ipv6-tunnel

Configure IPv6/IPv4 in IPv6 tunnel.

```
config system ipv6-tunnel
  Description: Configure IPv6/IPv4 in IPv6 tunnel.
  edit <name>
    set auto-asic-offload [enable|disable]
    set destination {ipv6-address}
    set interface {string}
    set source {ipv6-address}
  next
end
```

config system ipv6-tunnel

Parameter	Description	Type	Size
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-
		Option	Description
		<i>enable</i>	Enable auto ASIC offloading.
		<i>disable</i>	Disable ASIC offloading.
destination	Remote IPv6 address of the tunnel.	ipv6-address	Not Specified
interface	Interface name.	string	Maximum length: 15

Parameter	Description	Type	Size
name	IPv6 tunnel name.	string	Maximum length: 15
source	Local IPv6 address of the tunnel.	ipv6-address	Not Specified

* This parameter may not exist in some models.

config system isf-queue-profile



This command is available for model(s): FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3700D, FortiGate 5001D, FortiGate 800D.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Create a queue profile of switch.

```
config system isf-queue-profile
  Description: Create a queue profile of switch.
  edit <name>
    set bandwidth-unit [kbps|pps]
    set burst-control [disable|enable]
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
  next
end
```

config system isf-queue-profile

Parameter	Description	Type	Size
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth.	option	-
	Option	Description	
	<i>kbps</i>	kilobits per second.	
	<i>pps</i>	packets per second.	
burst-control	Burst control.	option	-
	Option	Description	
	<i>disable</i>	Disable burst control.	
	<i>enable</i>	Enable burst control.	
guaranteed-bandwidth	Guaranteed bandwidth.	integer	Minimum value: 0 Maximum value: 100000000
maximum-bandwidth	Upper bandwidth limit enforced.	integer	Minimum value: 0 Maximum value: 100000000
name	Profile name.	string	Maximum length: 15

config system link-monitor

Configure Link Health Monitor.

```
config system link-monitor
  Description: Configure Link Health Monitor.
  edit <name>
    set addr-mode [ipv4|ipv6]
    set failtime {integer}
    set gateway-ip {ipv4-address-any}
    set gateway-ip6 {ipv6-address}
    set ha-priority {integer}
    set http-agent {string}
    set http-get {string}
    set http-match {string}
    set interval {integer}
    set packet-size {integer}
```

```

set password {password}
set port {integer}
set probe-timeout {integer}
set protocol {option1}, {option2}, ...
set recoverytime {integer}
set security-mode [none|authentication]
set server <address1>, <address2>, ...
set source-ip {ipv4-address-any}
set source-ip6 {ipv6-address}
set srcintf {string}
set status [enable|disable]
set update-cascade-interface [enable|disable]
set update-static-route [enable|disable]
next
end

```

config system link-monitor

Parameter	Description	Type	Size						
addr-mode	Address mode (IPv4 or IPv6).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>	Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.		
	Option	Description							
	ipv4	IPv4 mode.							
ipv6	IPv6 mode.								
failtime	Number of retry attempts before the server is considered down (1 - 10, default = 5)	integer	Minimum value: 1 Maximum value: 3600						
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						
ha-priority	HA election priority (1 - 50).	integer	Minimum value: 1 Maximum value: 50						
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024						
http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.	string	Maximum length: 1024						
http-match	String that you expect to see in the HTTP-GET requests of the traffic to be monitored.	string	Maximum length: 1024						

Parameter	Description	Type	Size
interval	Detection interval in milliseconds (500 - 3600 * 1000 msec, default = 500).	integer	Minimum value: 500 Maximum value: 3600000
name	Link monitor name.	string	Maximum length: 35
packet-size	Packet size of a twamp test session,	integer	Minimum value: 64 Maximum value: 1024
password	Twamp controller password in authentication mode	password	Not Specified
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535
probe-timeout	Time to wait before a probe packet is considered lost (500 - 5000 msec, default = 500).	integer	Minimum value: 500 Maximum value: 5000
protocol	Protocols used to monitor the server.	option	-
	Option	Description	
	<i>ping</i>	PING link monitor.	
	<i>tcp-echo</i>	TCP echo link monitor.	
	<i>udp-echo</i>	UDP echo link monitor.	
	<i>http</i>	HTTP-GET link monitor.	
	<i>twamp</i>	TWAMP link monitor.	
	<i>ping6</i>	PING6 link monitor.	
recoverytime	Number of successful responses received before server is considered recovered (1 - 10, default = 5).	integer	Minimum value: 1 Maximum value: 3600
security-mode	Twamp controller security mode.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	Unauthenticated mode.	
	<i>authentication</i>	Authenticated mode.	
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79
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
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15
status	Enable/disable this link monitor.	option	-
	Option	Description	
	<i>enable</i>	Enable this link monitor.	
	<i>disable</i>	Disable this link monitor.	
update- cascade- interface	Enable/disable update cascade interface.	option	-
	Option	Description	
	<i>enable</i>	Enable update cascade interface.	
	<i>disable</i>	Disable update cascade interface.	
update-static- route	Enable/disable updating the static route.	option	-
	Option	Description	
	<i>enable</i>	Enable updating the static route.	
	<i>disable</i>	Disable updating the static route.	

config system lldp network-policy

Configure LLDP network policy.

```
config system lldp network-policy
  Description: Configure LLDP network policy.
  edit <name>
```

```
set comment {var-string}
config guest
    Description: Guest.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config guest-voice-signaling
    Description: Guest Voice Signaling.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config softphone
    Description: Softphone.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config streaming-video
    Description: Streaming Video.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config video-conferencing
    Description: Video Conferencing.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config video-signaling
    Description: Video Signaling.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
config voice
    Description: Voice.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
```

```

end
config voice-signaling
    Description: Voice signaling.
    set dscp {integer}
    set priority {integer}
    set status [disable|enable]
    set tag [none|dot1q|...]
    set vlan {integer}
end
next
end

```

config system lldp network-policy

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 1023
name	LLDP network policy name.	string	Maximum length: 35

config guest

Parameter	Description	Type	Size								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63								
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7								
status	Enable/disable advertising this policy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable advertising this LLDP network policy.</td></tr><tr><td><i>enable</i></td><td>Enable advertising this LLDP network policy.</td></tr></table>			Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.		
Option	Description										
<i>disable</i>	Disable advertising this LLDP network policy.										
<i>enable</i>	Enable advertising this LLDP network policy.										
tag	Advertise tagged or untagged traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Advertise that untagged frames should be used.</td></tr><tr><td><i>dot1q</i></td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td><i>dot1p</i></td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></table>			Option	Description	<i>none</i>	Advertise that untagged frames should be used.	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.
Option	Description										
<i>none</i>	Advertise that untagged frames should be used.										
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.										
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.										

Parameter	Description	Type	Size
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config guest-voice-signaling

Parameter	Description	Type	Size
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
status	Enable/disable advertising this policy.	option	-

Option	Description
<i>disable</i>	Disable advertising this LLDP network policy.
<i>enable</i>	Enable advertising this LLDP network policy.

tag	Advertise tagged or untagged traffic.	option	-

Option	Description
<i>none</i>	Advertise that untagged frames should be used.
<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.
<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.

vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config softphone

Parameter	Description	Type	Size
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63

Parameter	Description	Type	Size
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
status	Enable/disable advertising this policy.	option	-
	Option	Description	
	<i>disable</i>	Disable advertising this LLDP network policy.	
	<i>enable</i>	Enable advertising this LLDP network policy.	
tag	Advertise tagged or untagged traffic.	option	-
	Option	Description	
	<i>none</i>	Advertise that untagged frames should be used.	
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.	
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config streaming-video

Parameter	Description	Type	Size						
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63						
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7						
status	Enable/disable advertising this policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable advertising this LLDP network policy.</td></tr><tr><td><i>enable</i></td><td>Enable advertising this LLDP network policy.</td></tr></table>			Option	Description	<i>disable</i>	Disable advertising this LLDP network policy.	<i>enable</i>	Enable advertising this LLDP network policy.
Option	Description								
<i>disable</i>	Disable advertising this LLDP network policy.								
<i>enable</i>	Enable advertising this LLDP network policy.								
tag	Advertise tagged or untagged traffic.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	Advertise that untagged frames should be used.	
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.	
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config video-conferencing

Parameter	Description	Type	Size
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
status	Enable/disable advertising this policy.	option	-
	Option	Description	
	<i>disable</i>	Disable advertising this LLDP network policy.	
	<i>enable</i>	Enable advertising this LLDP network policy.	
tag	Advertise tagged or untagged traffic.	option	-
	Option	Description	
	<i>none</i>	Advertise that untagged frames should be used.	
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.	
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config video-signaling

Parameter	Description	Type	Size
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
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 (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config voice

Parameter	Description	Type	Size
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
status	Enable/disable advertising this policy.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable advertising this LLDP network policy.	
	<i>enable</i>	Enable advertising this LLDP network policy.	
tag	Advertise tagged or untagged traffic.	option	-
	Option	Description	
	<i>none</i>	Advertise that untagged frames should be used.	
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.	
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config voice-signaling

Parameter	Description	Type	Size
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63
priority	802.1P CoS/PCP to advertise (0 - 7; from lowest to highest priority).	integer	Minimum value: 0 Maximum value: 7
status	Enable/disable advertising this policy.	option	-
	Option	Description	
	<i>disable</i>	Disable advertising this LLDP network policy.	
	<i>enable</i>	Enable advertising this LLDP network policy.	
tag	Advertise tagged or untagged traffic.	option	-
	Option	Description	
	<i>none</i>	Advertise that untagged frames should be used.	
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.	
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.	

Parameter	Description	Type	Size
vlan	802.1Q VLAN ID to advertise (1 - 4094).	integer	Minimum value: 1 Maximum value: 4094

config system lte-modem



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64, FortiGateRugged 35D.

Configure USB LTE/WIMAX devices.

```
config system lte-modem
    Description: Configure USB LTE/WIMAX devices.
    set allow-modify-wireless-profile-table [enable|disable]
    set apn {string}
    set authtype [none|pap|...]
    set auto-connect [enable|disable]
    set band-restrictions {string}
    set billing-date {integer}
    set connection-hot-swap [5-minutes|10-minutes|...]
    set data-limit {integer}
    set data-usage-tracking [enable|disable]
    set extra-init {string}
    set force-wireless-profile {integer}
    set gps-port {integer}
```

```

set gps-service [enable|disable]
set holddown-timer {integer}
set image-preference [generic|att|...]
set interface {string}
set manual-handover [enable|disable]
set mode [standalone|redundant]
set modem-port {integer}
set network-type [auto|umts-3g|...]
set passwd {password}
set sim-hot-swap [enable|disable]
set sim-slot {integer}
set status [enable|disable]
set username {string}

```

end

config system lte-modem

Parameter	Description	Type	Size								
allow-modify-wireless-profile-table *	Allow LTE daemon to modify wireless profile table, if running GENERIC firmware.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow LTE daemon to modify wireless profile table.</td></tr><tr><td>disable</td><td>Do not allow LTE daemon to modify wireless profile table.</td></tr></table>	Option	Description	enable	Allow LTE daemon to modify wireless profile table.	disable	Do not allow LTE daemon to modify wireless profile table.				
Option	Description										
enable	Allow LTE daemon to modify wireless profile table.										
disable	Do not allow LTE daemon to modify wireless profile table.										
apn	Login APN string for PDP-IP packet data calls.	string	Maximum length: 127								
authtype	Authentication type for PDP-IP packet data calls.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Username and password not required.</td></tr><tr><td>pap</td><td>Use PAP authentication.</td></tr><tr><td>chap</td><td>Use CHAP authentication.</td></tr></table>	Option	Description	none	Username and password not required.	pap	Use PAP authentication.	chap	Use CHAP authentication.		
Option	Description										
none	Username and password not required.										
pap	Use PAP authentication.										
chap	Use CHAP authentication.										
auto-connect *	Enable/disable Modem auto connect.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable modem auto connect.</td></tr><tr><td>disable</td><td>Disable modem auto connect.</td></tr></table>	Option	Description	enable	Enable modem auto connect.	disable	Disable modem auto connect.				
Option	Description										
enable	Enable modem auto connect.										
disable	Disable modem auto connect.										
band-restrictions *	Bitmaps for the allowed 3G and LTE bands.Ex: 0000000000000000-0000000000001008 (3G Mask-LTE Mask)	string	Maximum length: 35								

Parameter	Description	Type	Size
billing-date *	LTE Modem billing date (1 - 31).	integer	Minimum value: 1 Maximum value: 31
connection-hot-swap *	Set connection-based SIM card hot swap time interval.	option	-
	Option	Description	
	5-minutes	Perform SIM card hot swapping if current card is not able to connect for 5 minutes.	
	10-minutes	Perform SIM card hot swapping if current card is not able to connect for 10 minutes.	
	never	SIM card hot swap based on card presence only.	
data-limit *	LTE Modem data limit (0 - 100000) mega bytes, 0 for unlimited data.	integer	Minimum value: 0 Maximum value: 100000
data-usage-tracking *	Enable/disable data usage tracking.	option	-
	Option	Description	
	enable	Enable data usage tracking.	
	disable	Disable data usage tracking.	
extra-init	Extra initialization string for USB LTE/WIMAX devices.	string	Maximum length: 127
force-wireless-profile *	Force to use wireless profile index (1 - 16), 0 if don't force.	integer	Minimum value: 0 Maximum value: 16
gps-port *	Modem GPS port index (0 - 20).	integer	Minimum value: 0 Maximum value: 20
gps-service *	Enable/disable GPS daemon.	option	-
	Option	Description	
	enable	Enable GPS daemon.	
	disable	Disable GPS daemon.	

Parameter	Description	Type	Size
holddown-timer	Hold down timer (10 - 60 sec).	integer	Minimum value: 10 Maximum value: 60
image-preference *	Modem Image Preference.	option	-

Option	Description
<i>generic</i>	Generic Firmware.
<i>att</i>	AT&T Firmware.
<i>verizon</i>	Verizon Firmware.
<i>telus</i>	Telus Firmware.
<i>docomo</i>	DOCOMO Firmware.
<i>softbank</i>	Softbank Firmware.
<i>sprint</i>	Sprint Firmware.
<i>auto-sim</i>	Auto Select Firmware.
<i>no-change</i>	Do not change.

interface	The interface that the modem is acting as a redundant interface for.	string	Maximum length: 63
manual-handover *	Enable/Disable manual handover from 3G to LTE network.	option	-

Option	Description
<i>enable</i>	Enable 3G to LTE manual handover.
<i>disable</i>	Disable 3G to LTE manual handover.

mode	Modem operation mode.	option	-

Option	Description
<i>standalone</i>	Standalone modem operation mode.
<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.

modem-port	Modem port index (0 - 20).	integer	Minimum value: 0 Maximum value: 20

Parameter	Description	Type	Size
network-type *	Set wireless network.	option	-
	Option	Description	
	<i>auto</i>	Automatic detection	
	<i>umts-3g</i>	UMTS 3G -- For networks use GSM technology	
	<i>lte</i>	LTE	
	<i>cdma-hrpd</i>	CDMA and HRPD -- For networks use CDMA technology	
passwd	Authentication password for PDP-IP packet data calls.	password	Not Specified
sim-hot-swap *	Enable/disable SIM card auto detection and hot swapping.	option	-
	Option	Description	
	<i>enable</i>	Enable SIM card auto detection.	
	<i>disable</i>	Disable SIM card auto detection.	
sim-slot *	SIM card slot (1 - 2). 1: right slot. 2: left slot.	integer	Minimum value: 1 Maximum value: 2
status	Enable/disable USB LTE/WIMAX device.	option	-
	Option	Description	
	<i>enable</i>	Enable USB LTE/WIMA device.	
	<i>disable</i>	Disable USB LTE/WIMA device.	
username	Authentication username for PDP-IP packet data calls.	string	Maximum length: 63

* This parameter may not exist in some models.

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
mac	MAC address.	mac-address	Not Specified
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified

config system management-tunnel

Management tunnel configuration.

```
config system management-tunnel
    Description: Management tunnel configuration.
    set allow-collect-statistics [enable|disable]
    set allow-config-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set authorized-manager-only [enable|disable]
    set serial-number {user}
    set status [enable|disable]
end
```

config system management-tunnel

Parameter	Description	Type	Size
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-
	Option	Description	
	<i>enable</i>	Enable collection of run time statistics.	
	<i>disable</i>	Disable collection of run time statistics.	
allow-config-restore	Enable/disable allow config restore.	option	-
	Option	Description	
	<i>enable</i>	Enable allow config restore.	
	<i>disable</i>	Disable allow config restore.	
allow-push-configuration	Enable/disable push configuration.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable push configuration.	
	<i>disable</i>	Disable push configuration.	
allow-push-firmware	Enable/disable push firmware.	option	-
	Option	Description	
	<i>enable</i>	Enable push firmware.	
	<i>disable</i>	Disable push firmware.	
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-
	Option	Description	
	<i>enable</i>	Enable restriction of authorized manager only.	
	<i>disable</i>	Disable restriction of authorized manager only.	
serial-number	Serial number.	user	Not Specified
status	Enable/disable FGFM tunnel.	option	-
	Option	Description	
	<i>enable</i>	Enable management tunnel.	
	<i>disable</i>	Disable management tunnel.	

config system mobile-tunnel

Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.

```

config system mobile-tunnel
    Description: Configure Mobile tunnels, an implementation of Network Mobility (NEMO)
    extensions for Mobile IPv4 RFC5177.
    edit <name>
        set hash-algorithm {option}
        set home-address {ipv4-address}
        set home-agent {ipv4-address}
        set lifetime {integer}
        set n-mhae-key {user}
        set n-mhae-key-type [ascii|base64]
        set n-mhae-spi {integer}
    config network
        Description: NEMO network configuration.
        edit <id>

```

```

        set interface {string}
        set prefix {ipv4-classnet}
    next
end
set reg-interval {integer}
set reg-retry {integer}
set renew-interval {integer}
set roaming-interface {string}
set status [disable|enable]
set tunnel-mode {option}
next
end

```

config system mobile-tunnel

Parameter	Description	Type	Size
hash-algorithm	Hash Algorithm (Keyed MD5).	option	-
	Option	Description	
	<i>hmac-md5</i>	Keyed MD5.	
home-address	Home IP address (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
home-agent	IPv4 address of the NEMO HA (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified
lifetime	NMMO HA registration request lifetime (180 - 65535 sec, default = 65535).	integer	Minimum value: 180 Maximum value: 65535
n-mhae-key	NEMO authentication key.	user	Not Specified
n-mhae-key-type	NEMO authentication key type (ascii or base64).	option	-
	Option	Description	
	<i>ascii</i>	The authentication key is an ASCII string.	
	<i>base64</i>	The authentication key is Base64 encoded.	
n-mhae-spi	NEMO authentication SPI (default: 256).	integer	Minimum value: 0 Maximum value: 4294967295
name	Tunnel name.	string	Maximum length: 15

Parameter	Description	Type	Size						
reg-interval	NMMO HA registration interval (5 - 300, default = 5).	integer	Minimum value: 5 Maximum value: 300						
reg-retry	Maximum number of NMMO HA registration retries (1 to 30, default = 3).	integer	Minimum value: 1 Maximum value: 30						
renew-interval	Time before lifetime expiration to send NMMO HA re-registration (5 - 60, default = 60).	integer	Minimum value: 5 Maximum value: 60						
roaming-interface	Select the associated interface name from available options.	string	Maximum length: 15						
status	Enable/disable this mobile tunnel.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this mobile tunnel.</td></tr><tr><td><i>enable</i></td><td>Enable this mobile tunnel.</td></tr></table>			Option	Description	<i>disable</i>	Disable this mobile tunnel.	<i>enable</i>	Enable this mobile tunnel.
Option	Description								
<i>disable</i>	Disable this mobile tunnel.								
<i>enable</i>	Enable this mobile tunnel.								
tunnel-mode	NEMO tunnel mode (GRE tunnel).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>gre</i></td><td>GRE tunnel.</td></tr></table>			Option	Description	<i>gre</i>	GRE tunnel.		
Option	Description								
<i>gre</i>	GRE tunnel.								

config network

Parameter	Description	Type	Size
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
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 modem



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate-VM64, FortiGateRugged 35D.

Configure MODEM.

```
config system modem
  Description: Configure MODEM.
  set action [dial|stop|...]
  set altmode [enable|disable]
  set authtype1 {option1}, {option2}, ...
  set authtype2 {option1}, {option2}, ...
  set authtype3 {option1}, {option2}, ...
  set auto-dial [enable|disable]
  set connect-timeout {integer}
  set dial-cmd1 {string}
  set dial-cmd2 {string}
  set dial-cmd3 {string}
  set dial-on-demand [enable|disable]
  set distance {integer}
  set dont-send-CR1 [enable|disable]
  set dont-send-CR2 [enable|disable]
  set dont-send-CR3 [enable|disable]
  set extra-init1 {string}
  set extra-init2 {string}
  set extra-init3 {string}
  set holddown-timer {integer}
  set idle-timer {integer}
  set interface {string}
```

```

set lockdown-lac {string}
set mode [standalone|redundant]
set network-init {string}
set passwd1 {password}
set passwd2 {password}
set passwd3 {password}
set peer-modem1 [generic|actiontec|...]
set peer-modem2 [generic|actiontec|...]
set peer-modem3 [generic|actiontec|...]
set phone1 {string}
set phone2 {string}
set phone3 {string}
set pin-init {string}
set ppp-echo-request1 [enable|disable]
set ppp-echo-request2 [enable|disable]
set ppp-echo-request3 [enable|disable]
set priority {integer}
set redial [none|1|...]
set reset {integer}
set status [enable|disable]
set traffic-check [enable|disable]
set username1 {string}
set username2 {string}
set username3 {string}
set wireless-port {integer}
end

```

end

config system modem

Parameter	Description	Type	Size
action	Dial up/stop MODEM.	option	-
	Option	Description	
	<i>dial</i>	Dial up number.	
	<i>stop</i>	Stop dialup.	
	<i>none</i>	No action.	
altmode	Enable/disable altmode for installations using PPP in China.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
authtype1	Allowed authentication types for ISP 1.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr><tr><td><i>mschap</i></td><td>MSCHAP</td></tr><tr><td><i>mschapv2</i></td><td>MSCHAPv2</td></tr></table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2		
	Option	Description											
	<i>pap</i>	PAP											
	<i>chap</i>	CHAP											
	<i>mschap</i>	MSCHAP											
	<i>mschapv2</i>	MSCHAPv2											
authtype2	Allowed authentication types for ISP 2.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr><tr><td><i>mschap</i></td><td>MSCHAP</td></tr><tr><td><i>mschapv2</i></td><td>MSCHAPv2</td></tr></table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2		
	Option	Description											
	<i>pap</i>	PAP											
	<i>chap</i>	CHAP											
	<i>mschap</i>	MSCHAP											
	<i>mschapv2</i>	MSCHAPv2											
authtype3	Allowed authentication types for ISP 3.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pap</i></td><td>PAP</td></tr><tr><td><i>chap</i></td><td>CHAP</td></tr><tr><td><i>mschap</i></td><td>MSCHAP</td></tr><tr><td><i>mschapv2</i></td><td>MSCHAPv2</td></tr></table>	Option	Description	<i>pap</i>	PAP	<i>chap</i>	CHAP	<i>mschap</i>	MSCHAP	<i>mschapv2</i>	MSCHAPv2		
	Option	Description											
	<i>pap</i>	PAP											
	<i>chap</i>	CHAP											
	<i>mschap</i>	MSCHAP											
	<i>mschapv2</i>	MSCHAPv2											
auto-dial	Enable/disable auto-dial after a reboot or disconnection.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
	<i>disable</i>	Disable setting.											
connect-timeout	Connection completion timeout (30 - 255 sec, default = 90).	integer	Minimum value: 30 Maximum value: 255										
dial-cmd1	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63										
dial-cmd2	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63										

Parameter	Description	Type	Size						
dial-cmd3	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63						
dial-on-demand	Enable/disable to dial the modem when packets are routed to the modem interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
distance	Distance of learned routes (1 - 255, default = 1).	integer	Minimum value: 1 Maximum value: 255						
dont-send-CR1	Do not send CR when connected (ISP1).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
dont-send-CR2	Do not send CR when connected (ISP2).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
dont-send-CR3	Do not send CR when connected (ISP3).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
extra-init1	Extra initialization string to ISP 1.	string	Maximum length: 127						
extra-init2	Extra initialization string to ISP 2.	string	Maximum length: 127						
extra-init3	Extra initialization string to ISP 3.	string	Maximum length: 127						

Parameter	Description	Type	Size
holddown-timer	Hold down timer in seconds (1 - 60 sec).	integer	Minimum value: 1 Maximum value: 60
idle-timer	MODEM connection idle time (1 - 9999 min, default = 5).	integer	Minimum value: 1 Maximum value: 9999
interface	Name of redundant interface.	string	Maximum length: 63
lockdown-lac	Allow connection only to the specified Location Area Code (LAC).	string	Maximum length: 127
mode	Set MODEM operation mode to redundant or standalone.	option	-

Option	Description
<i>standalone</i>	Standalone.
<i>redundant</i>	Redundant for an interface.

network-init	AT command to set the Network name/type (AT+COPS=<mode>,[<format>,<oper>[,<AcT>]]).	string	Maximum length: 127
passwd1	Password to access the specified dialup account.	password	Not Specified
passwd2	Password to access the specified dialup account.	password	Not Specified
passwd3	Password to access the specified dialup account.	password	Not Specified
peer-modem1	Specify peer MODEM type for phone1.	option	-

Option	Description
<i>generic</i>	All other modem type.
<i>actiontec</i>	ActionTec modem.
<i>ascend_TNT</i>	Ascend TNT modem.

peer-modem2	Specify peer MODEM type for phone2.	option	-

Option	Description
<i>generic</i>	All other modem type.
<i>actiontec</i>	ActionTec modem.
<i>ascend_TNT</i>	Ascend TNT modem.

Parameter	Description	Type	Size
peer-modem3	Specify peer MODEM type for phone3.	option	-

Option	Description
<i>generic</i>	All other modem type.
<i>actiontec</i>	ActionTec modem.
<i>ascend_TNT</i>	Ascend TNT modem.

phone1	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63
phone2	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63
phone3	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63
pin-init	AT command to set the PIN (AT+PIN=<pin>).	string	Maximum length: 127
ppp-echo-request1	Enable/disable PPP echo-request to ISP 1.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

ppp-echo-request2	Enable/disable PPP echo-request to ISP 2.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

ppp-echo-request3	Enable/disable PPP echo-request to ISP 3.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

Parameter	Description	Type	Size
priority	Priority of learned routes (0 - 4294967295, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295
redial	Redial limit (1 - 10 attempts, none = redial forever).	option	-

Option	Description
<i>none</i>	Forever.
<i>1</i>	One attempt.
<i>2</i>	Two attempts.
<i>3</i>	Three attempts.
<i>4</i>	Four attempts.
<i>5</i>	Five attempts.
<i>6</i>	Six attempts.
<i>7</i>	Seven attempts.
<i>8</i>	Eight attempts.
<i>9</i>	Nine attempts.
<i>10</i>	Ten attempts.

reset	Number of dial attempts before resetting modem (0 = never reset).	integer	Minimum value: 0 Maximum value: 10
status	Enable/disable Modem support (equivalent to bringing an interface up or down).	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

traffic-check	Enable/disable traffic-check.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

Parameter	Description	Type	Size
username1	User name to access the specified dialup account.	string	Maximum length: 63
username2	User name to access the specified dialup account.	string	Maximum length: 63
username3	User name to access the specified dialup account.	string	Maximum length: 63
wireless-port	Enter wireless port number, 0 for default, 1 for first port, ... (0 - 4294967295, default = 0)	integer	Minimum value: 0 Maximum value: 4294967295

config system nat64

Configure NAT64.

```
config system nat64
    Description: Configure NAT64.
    set always-synthesize-aaaa-record [enable|disable]
    set generate-ipv6-fragment-header [enable|disable]
    set nat46-force-ipv4-packet-forwarding [enable|disable]
    set nat64-prefix {ipv6-prefix}
    config secondary-prefix
        Description: Secondary NAT64 prefix.
        edit <name>
            set nat64-prefix {ipv6-prefix}
        next
    end
    set secondary-prefix-status [enable|disable]
    set status [enable|disable]
end
```

config system nat64

Parameter	Description	Type	Size
always-synthesize-aaaa-record	Enable/disable AAAA record synthesis (default = enable).	option	-
Option	Description		
<i>enable</i>	Enable AAAA record synthesis.		
<i>disable</i>	Disable AAAA record synthesis.		

Parameter	Description	Type	Size						
generate-ipv6-fragment-header	Enable/disable IPv6 fragment header generation.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPv6 fragment header generation.</td></tr><tr><td><i>disable</i></td><td>Disable IPv6 fragment header generation.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPv6 fragment header generation.	<i>disable</i>	Disable IPv6 fragment header generation.		
Option	Description								
<i>enable</i>	Enable IPv6 fragment header generation.								
<i>disable</i>	Disable IPv6 fragment header generation.								
nat46-force-ipv4-packet-forwarding	Enable/disable mandatory IPv4 packet forwarding in nat46.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr><tr><td><i>disable</i></td><td>Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr></table>	Option	Description	<i>enable</i>	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.	<i>disable</i>	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.		
Option	Description								
<i>enable</i>	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.								
<i>disable</i>	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.								
nat64-prefix	NAT64 prefix must be ::/96 (default = 64:ff9b::/96).	ipv6-prefix	Not Specified						
secondary-prefix-status	Enable/disable secondary NAT64 prefix.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secondary NAT64.</td></tr><tr><td><i>disable</i></td><td>Disable secondary NAT64.</td></tr></table>	Option	Description	<i>enable</i>	Enable secondary NAT64.	<i>disable</i>	Disable secondary NAT64.		
Option	Description								
<i>enable</i>	Enable secondary NAT64.								
<i>disable</i>	Disable secondary NAT64.								
status	Enable/disable NAT64 (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAT64.</td></tr><tr><td><i>disable</i></td><td>Disable NAT64.</td></tr></table>	Option	Description	<i>enable</i>	Enable NAT64.	<i>disable</i>	Disable NAT64.		
Option	Description								
<i>enable</i>	Enable NAT64.								
<i>disable</i>	Disable NAT64.								

config secondary-prefix

Parameter	Description	Type	Size
name	NAT64 prefix name.	string	Maximum length: 35
nat64-prefix	NAT64 prefix.	ipv6-prefix	Not Specified

config system nd-proxy

Configure IPv6 neighbor discovery proxy (RFC4389).

```

config system nd-proxy
    Description: Configure IPv6 neighbor discovery proxy (RFC4389).
    set member <interface-name1>, <interface-name2>, ...
    set status [enable|disable]
end

```

config system nd-proxy

Parameter	Description	Type	Size						
member <interface-name>	Interfaces using the neighbor discovery proxy. Interface name.	string	Maximum length: 79						
status	Enable/disable neighbor discovery proxy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable neighbor discovery proxy.</td></tr><tr><td>disable</td><td>Disable neighbor discovery proxy.</td></tr></table>			Option	Description	enable	Enable neighbor discovery proxy.	disable	Disable neighbor discovery proxy.
Option	Description								
enable	Enable neighbor discovery proxy.								
disable	Disable neighbor discovery proxy.								

config system netflow

Configure NetFlow.

```

config system netflow
    Description: Configure NetFlow.
    set active-flow-timeout {integer}
    set collector-ip {ipv4-address}
    set collector-port {integer}
    set inactive-flow-timeout {integer}
    set source-ip {ipv4-address}
    set template-tx-counter {integer}
    set template-tx-timeout {integer}
end

```

config system netflow

Parameter	Description	Type	Size
active-flow-timeout	Timeout to report active flows (1 - 60 min, default = 30).	integer	Minimum value: 1 Maximum value: 60
collector-ip	Collector IP.	ipv4-address	Not Specified

Parameter	Description	Type	Size
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535
inactive-flow-timeout	Timeout for periodic report of finished flows (10 - 600 sec, default = 15).	integer	Minimum value: 10 Maximum value: 600
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified
template-tx-counter	Counter of flowset records before resending a template flowset record.	integer	Minimum value: 10 Maximum value: 6000
template-tx-timeout	Timeout for periodic template flowset transmission (1 - 1440 min, default = 30).	integer	Minimum value: 1 Maximum value: 1440

config system network-visibility

Configure network visibility settings.

```
config system network-visibility
    Description: Configure network visibility settings.
    set destination-hostname-visibility [disable|enable]
    set destination-location [disable|enable]
    set destination-visibility [disable|enable]
    set hostname-limit {integer}
    set hostname-ttl {integer}
    set source-location [disable|enable]
end
```

config system network-visibility

Parameter	Description	Type	Size
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-
	Option	Description	
	<i>disable</i>	Disable logging of destination hostname visibility.	
	<i>enable</i>	Enable logging of destination hostname visibility.	

Parameter	Description	Type	Size
destination-location	Enable/disable logging of destination geographical location visibility.	option	-

Option	Description
<i>disable</i>	Disable logging of destination geographical location visibility.
<i>enable</i>	Enable logging of destination geographical location visibility.

destination-visibility	Enable/disable logging of destination visibility.	option	-

Option	Description
<i>disable</i>	Disable logging of destination visibility.
<i>enable</i>	Enable logging of destination visibility.

hostname-limit	Limit of the number of hostname table entries (0 - 50000).	integer	Minimum value: 0 Maximum value: 50000

hostname-ttl	TTL of hostname table entries (60 - 86400).	integer	Minimum value: 60 Maximum value: 86400

source-location	Enable/disable logging of source geographical location visibility.	option	-

Option	Description
<i>disable</i>	Disable logging of source geographical location visibility.
<i>enable</i>	Enable logging of source geographical location visibility.

config system np6



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 201E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NP6 attributes.

```
config system np6
    Description: Configure NP6 attributes.
    edit <name>
        set fastpath [disable|enable]
        config fp-anomaly
            Description: NP6 IPv4 anomaly protection. trap-to-host forwards anomaly sessions
            to the CPU.
            set icmp-csum-err [drop|trap-to-host]
            set icmp-frag [allow|drop|...]
            set icmp-land [allow|drop|...]
            set ipv4-csum-err [drop|trap-to-host]
            set ipv4-land [allow|drop|...]
            set ipv4-optlsrr [allow|drop|...]
            set ipv4-optrr [allow|drop|...]
            set ipv4-optsecurity [allow|drop|...]
            set ipv4-optssrr [allow|drop|...]
            set ipv4-optstream [allow|drop|...]
            set ipv4-opttimestamp [allow|drop|...]
            set ipv4-proto-err [allow|drop|...]
            set ipv4-unknopt [allow|drop|...]
            set ipv6-daddr-err [allow|drop|...]
            set ipv6-land [allow|drop|...]
            set ipv6-optendpid [allow|drop|...]
```

```

        set ipv6-opthomeaddr [allow|drop|...]
        set ipv6-optinvald [allow|drop|...]
        set ipv6-optjumbo [allow|drop|...]
        set ipv6-optnsap [allow|drop|...]
        set ipv6-optralert [allow|drop|...]
        set ipv6-opttunnel [allow|drop|...]
        set ipv6-proto-err [allow|drop|...]
        set ipv6-saddr-err [allow|drop|...]
        set ipv6-unknopt [allow|drop|...]
        set tcp-csum-err [drop|trap-to-host]
        set tcp-fin-noack [allow|drop|...]
        set tcp-fin-only [allow|drop|...]
        set tcp-land [allow|drop|...]
        set tcp-no-flag [allow|drop|...]
        set tcp-syn-data [allow|drop|...]
        set tcp-syn-fin [allow|drop|...]
        set tcp-winnuke [allow|drop|...]
        set udp-csum-err [drop|trap-to-host]
        set udp-land [allow|drop|...]
    end
    set garbage-session-collector [disable|enable]
    config hpe
        Description: HPE configuration.
        set arp-max {integer}
        set enable-shaper [disable|enable]
        set esp-max {integer}
        set icmp-max {integer}
        set ip-frag-max {integer}
        set ip-others-max {integer}
        set l2-others-max {integer}
        set pri-type-max {integer}
        set sctp-max {integer}
        set tcp-max {integer}
        set tcpfin-rst-max {integer}
        set tcpsyn-ack-max {integer}
        set tcpsyn-max {integer}
        set udp-max {integer}
    end
    set ipsec-ob-hash-function [switch-group-hash|global-hash|...]
    set ipsec-outbound-hash [disable|enable]
    set low-latency-mode [disable|enable]
    set per-session-accounting [disable|traffic-log-only|...]
    set session-collector-interval {integer}
    set session-timeout-fixed [disable|enable]
    set session-timeout-interval {integer}
    set session-timeout-random-range {integer}
next
end

```

config system np6

Parameter	Description	Type	Size
fastpath	Enable/disable NP4 or NP6 offloading (also called fast path).	option	-
	Option	Description	
	<i>disable</i>	Disable NP4 or NP6 offloading (fast path).	
	<i>enable</i>	Enable NP4 or NP6 offloading (fast path).	
garbage-session-collector	Enable/disable garbage session collector.	option	-
	Option	Description	
	<i>disable</i>	Disable garbage session collector.	
	<i>enable</i>	Enable garbage session collector.	
ipsec-ob-hash-function *	Set hash function for IPsec outbound.	option	-
	Option	Description	
	<i>switch-group-hash</i>	Hash outbound SA traffic within NPs connected to same switch.	
	<i>global-hash</i>	Hash outbound SA traffic among all NPs.	
	<i>global-hash-weighted</i>	Hash outbound SA traffic among all NPs with more weights on NPs connected to switch 0. It's applicable to the case that ingress traffic is from switch 1.	
	<i>round-robin-switch-group</i>	Round-robin outbound SA traffic within NPs connected to same switch.	
	<i>round-robin-global</i>	Round-robin outbound SA traffic among all NPs.	
ipsec-outbound-hash *	Enable/disable hash function for IPsec outbound traffic.	option	-
	Option	Description	
	<i>disable</i>	Disable hash function for IPsec outbound traffic.	
	<i>enable</i>	Enable hash function for IPsec outbound traffic.	

Parameter	Description	Type	Size								
low-latency-mode	Enable/disable low latency mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable low latency mode.</td></tr><tr><td><i>enable</i></td><td>Enable low latency mode.</td></tr></table>	Option	Description	<i>disable</i>	Disable low latency mode.	<i>enable</i>	Enable low latency mode.				
Option	Description										
<i>disable</i>	Disable low latency mode.										
<i>enable</i>	Enable low latency mode.										
name	Device Name.	string	Maximum length: 31								
per-session-accounting	Enable/disable per-session accounting.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per-session accounting.</td></tr><tr><td><i>traffic-log-only</i></td><td>Per-session accounting only for sessions with traffic logging enable firewall policy.</td></tr><tr><td><i>enable</i></td><td>Per-session accounting for all sessions.</td></tr></table>	Option	Description	<i>disable</i>	Disable per-session accounting.	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enable firewall policy.	<i>enable</i>	Per-session accounting for all sessions.		
Option	Description										
<i>disable</i>	Disable per-session accounting.										
<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enable firewall policy.										
<i>enable</i>	Per-session accounting for all sessions.										
session-collector-interval	Set garbage session collection cleanup interval (1 - 100 sec, default 64).	integer	Minimum value: 1 Maximum value: 100								
session-timeout-fixed	{disable enable} Toggle between using fixed or random timeouts for refreshing NP6 sessions.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Refresh NP6 sessions at the configured fixed interval.</td></tr><tr><td><i>enable</i></td><td>Enable Refresh NP6 sessions randomly where the time between re within the random range.</td></tr></table>	Option	Description	<i>disable</i>	Disable Refresh NP6 sessions at the configured fixed interval.	<i>enable</i>	Enable Refresh NP6 sessions randomly where the time between re within the random range.				
Option	Description										
<i>disable</i>	Disable Refresh NP6 sessions at the configured fixed interval.										
<i>enable</i>	Enable Refresh NP6 sessions randomly where the time between re within the random range.										
session-timeout-interval	Set the fixed timeout for refreshing NP6 sessions (0 - 1000 sec, default 40 sec).	integer	Minimum value: 0 Maximum value: 1000								
session-timeout-random-range	Set the random timeout range for refreshing NP6 sessions (0 - 1000 sec, default 8 sec).	integer	Minimum value: 0 Maximum value: 1000								

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size								
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid ICMP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid ICMP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid ICMP checksum.	trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.				
Option	Description										
drop	Drop IPv4 invalid ICMP checksum.										
trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.										
icmp-frag	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow L3 fragment packet with L4 protocol as ICMP attack to pass.</td></tr><tr><td>drop</td><td>Drop L3 fragment packet with L4 protocol as ICMP attack.</td></tr><tr><td>trap-to-host</td><td>Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.	drop	Drop L3 fragment packet with L4 protocol as ICMP attack.	trap-to-host	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.		
Option	Description										
allow	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.										
drop	Drop L3 fragment packet with L4 protocol as ICMP attack.										
trap-to-host	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.										
icmp-land	ICMP land anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow ICMP land attack to pass.</td></tr><tr><td>drop</td><td>Drop ICMP land attack.</td></tr><tr><td>trap-to-host</td><td>Forward ICMP land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow ICMP land attack to pass.	drop	Drop ICMP land attack.	trap-to-host	Forward ICMP land attack to FortiOS.		
Option	Description										
allow	Allow ICMP land attack to pass.										
drop	Drop ICMP land attack.										
trap-to-host	Forward ICMP land attack to FortiOS.										
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid IP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid IP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid IP checksum.	trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.				
Option	Description										
drop	Drop IPv4 invalid IP checksum.										
trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.										
ipv4-land	Land anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 land attack to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 land attack.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 land attack to pass.	drop	Drop IPv4 land attack.	trap-to-host	Forward IPv4 land attack to FortiOS.		
Option	Description										
allow	Allow IPv4 land attack to pass.										
drop	Drop IPv4 land attack.										
trap-to-host	Forward IPv4 land attack to FortiOS.										
ipv4-optlrr	Loose source record route option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with loose source record route option to pass.</td></tr></table>	Option	Description	allow	Allow IPv4 with loose source record route option to pass.						
Option	Description										
allow	Allow IPv4 with loose source record route option to pass.										

Parameter	Description	Type	Size
	Option	Description	
	<i>drop</i>	Drop IPv4 with loose source record route option.	
	<i>trap-to-host</i>	Forward IPv4 with loose source record route option to FortiOS.	
ipv4-optrr	Record route option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with record route option to pass.	
	<i>drop</i>	Drop IPv4 with record route option.	
	<i>trap-to-host</i>	Forward IPv4 with record route option to FortiOS.	
ipv4-optsecurity	Security option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with security option to pass.	
	<i>drop</i>	Drop IPv4 with security option.	
	<i>trap-to-host</i>	Forward IPv4 with security option to FortiOS.	
ipv4-optssrr	Strict source record route option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with strict source record route option to pass.	
	<i>drop</i>	Drop IPv4 with strict source record route option.	
	<i>trap-to-host</i>	Forward IPv4 with strict source record route option to FortiOS.	
ipv4-optstream	Stream option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with stream option to pass.	
	<i>drop</i>	Drop IPv4 with stream option.	
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.	
ipv4-opttimestamp	Timestamp option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with timestamp option to pass.	
	<i>drop</i>	Drop IPv4 with timestamp option.	

Parameter	Description	Type	Size
	Option	Description	
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.	
ipv4-proto-err	Invalid layer 4 protocol anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 invalid L4 protocol to pass.	
	<i>drop</i>	Drop IPv4 invalid L4 protocol.	
	<i>trap-to-host</i>	Forward IPv4 invalid L4 protocol to FortiOS.	
ipv4-unknpt	Unknown option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with unknown options to pass.	
	<i>drop</i>	Drop IPv4 with unknown options.	
	<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.	
ipv6-daddr-err	Destination address as unspecified or loopback address anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 with destination address as unspecified or loopback address to pass.	
	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.	
	<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.	
ipv6-land	Land anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 land attack to pass.	
	<i>drop</i>	Drop IPv6 land attack.	
	<i>trap-to-host</i>	Forward IPv6 land attack to FortiOS.	
ipv6-optendpid	End point identification anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 with end point identification option to pass.	

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv6 with end point identification option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with end point identification option to FortiOS.</td></tr></table>	Option	Description	drop	Drop IPv6 with end point identification option.	trap-to-host	Forward IPv6 with end point identification option to FortiOS.				
	Option	Description									
	drop	Drop IPv6 with end point identification option.									
trap-to-host	Forward IPv6 with end point identification option to FortiOS.										
ipv6-opthomeaddr	Home address option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with home address option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with home address option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with home address option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with home address option to pass.	drop	Drop IPv6 with home address option.	trap-to-host	Forward IPv6 with home address option to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with home address option to pass.									
	drop	Drop IPv6 with home address option.									
trap-to-host	Forward IPv6 with home address option to FortiOS.										
ipv6-optinvald	Invalid option anomalies.Invalid option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with invalid option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with invalid option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with invalid option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with invalid option to pass.	drop	Drop IPv6 with invalid option.	trap-to-host	Forward IPv6 with invalid option to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with invalid option to pass.									
	drop	Drop IPv6 with invalid option.									
trap-to-host	Forward IPv6 with invalid option to FortiOS.										
ipv6-optjumbo	Jumbo options anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with jumbo option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with jumbo option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with jumbo option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with jumbo option to pass.	drop	Drop IPv6 with jumbo option.	trap-to-host	Forward IPv6 with jumbo option to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with jumbo option to pass.									
	drop	Drop IPv6 with jumbo option.									
trap-to-host	Forward IPv6 with jumbo option to FortiOS.										
ipv6-optnsap	Network service access point address option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with network service access point address option to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with network service access point address option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with network service access point address option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with network service access point address option to pass.	drop	Drop IPv6 with network service access point address option.	trap-to-host	Forward IPv6 with network service access point address option to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with network service access point address option to pass.									
	drop	Drop IPv6 with network service access point address option.									
trap-to-host	Forward IPv6 with network service access point address option to FortiOS.										
ipv6-optralert	Router alert option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with router alert option to pass.</td></tr></table>	Option	Description	allow	Allow IPv6 with router alert option to pass.						
	Option	Description									
allow	Allow IPv6 with router alert option to pass.										

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv6 with router alert option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with router alert option to FortiOS.</td></tr></table>	Option	Description	drop	Drop IPv6 with router alert option.	trap-to-host	Forward IPv6 with router alert option to FortiOS.				
	Option	Description									
	drop	Drop IPv6 with router alert option.									
trap-to-host	Forward IPv6 with router alert option to FortiOS.										
ipv6-opttunnel	Tunnel encapsulation limit option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with tunnel encapsulation limit to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with tunnel encapsulation limit.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with tunnel encapsulation limit to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with tunnel encapsulation limit to pass.	drop	Drop IPv6 with tunnel encapsulation limit.	trap-to-host	Forward IPv6 with tunnel encapsulation limit to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with tunnel encapsulation limit to pass.									
	drop	Drop IPv6 with tunnel encapsulation limit.									
trap-to-host	Forward IPv6 with tunnel encapsulation limit to FortiOS.										
ipv6-proto-err	Layer 4 invalid protocol anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 L4 invalid protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 L4 invalid protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 L4 invalid protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 L4 invalid protocol to pass.	drop	Drop IPv6 L4 invalid protocol.	trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.		
	Option	Description									
	allow	Allow IPv6 L4 invalid protocol to pass.									
	drop	Drop IPv6 L4 invalid protocol.									
trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.										
ipv6-saddr-err	Source address as multicast anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with source address as multicast to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with source address as multicast.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with source address as multicast to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with source address as multicast to pass.	drop	Drop IPv6 with source address as multicast.	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with source address as multicast to pass.									
	drop	Drop IPv6 with source address as multicast.									
trap-to-host	Forward IPv6 with source address as multicast to FortiOS.										
ipv6-unknpt	Unknown option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with unknown options to pass.	drop	Drop IPv6 with unknown options.	trap-to-host	Forward IPv6 with unknown options to FortiOS.		
	Option	Description									
	allow	Allow IPv6 with unknown options to pass.									
	drop	Drop IPv6 with unknown options.									
trap-to-host	Forward IPv6 with unknown options to FortiOS.										
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid TCP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid TCP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid TCP checksum.	trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.				
	Option	Description									
	drop	Drop IPv4 invalid TCP checksum.									
trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.										

Parameter	Description	Type	Size								
tcp-fin-noack	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow TCP packets with FIN flag set without ack setting to pass.</td></tr><tr><td><i>drop</i></td><td>Drop TCP packets with FIN flag set without ack setting.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward TCP packets with FIN flag set without ack setting to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow TCP packets with FIN flag set without ack setting to pass.	<i>drop</i>	Drop TCP packets with FIN flag set without ack setting.	<i>trap-to-host</i>	Forward TCP packets with FIN flag set without ack setting to FortiOS.		
Option	Description										
<i>allow</i>	Allow TCP packets with FIN flag set without ack setting to pass.										
<i>drop</i>	Drop TCP packets with FIN flag set without ack setting.										
<i>trap-to-host</i>	Forward TCP packets with FIN flag set without ack setting to FortiOS.										
tcp-fin-only	TCP SYN flood with only FIN flag set anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow TCP packets with FIN flag set only to pass.</td></tr><tr><td><i>drop</i></td><td>Drop TCP packets with FIN flag set only.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward TCP packets with FIN flag set only to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow TCP packets with FIN flag set only to pass.	<i>drop</i>	Drop TCP packets with FIN flag set only.	<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.		
Option	Description										
<i>allow</i>	Allow TCP packets with FIN flag set only to pass.										
<i>drop</i>	Drop TCP packets with FIN flag set only.										
<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.										
tcp-land	TCP land anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow TCP land attack to pass.</td></tr><tr><td><i>drop</i></td><td>Drop TCP land attack.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward TCP land attack to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow TCP land attack to pass.	<i>drop</i>	Drop TCP land attack.	<i>trap-to-host</i>	Forward TCP land attack to FortiOS.		
Option	Description										
<i>allow</i>	Allow TCP land attack to pass.										
<i>drop</i>	Drop TCP land attack.										
<i>trap-to-host</i>	Forward TCP land attack to FortiOS.										
tcp-no-flag	TCP SYN flood with no flag set anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow TCP packets without flag set to pass.</td></tr><tr><td><i>drop</i></td><td>Drop TCP packets without flag set.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward TCP packets without flag set to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow TCP packets without flag set to pass.	<i>drop</i>	Drop TCP packets without flag set.	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.		
Option	Description										
<i>allow</i>	Allow TCP packets without flag set to pass.										
<i>drop</i>	Drop TCP packets without flag set.										
<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.										
tcp-syn-data	TCP SYN flood packets with data anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow TCP syn packets with data to pass.</td></tr><tr><td><i>drop</i></td><td>Drop TCP syn packets with data.</td></tr><tr><td><i>trap-to-host</i></td><td>Forward TCP syn packets with data to FortiOS.</td></tr></table>	Option	Description	<i>allow</i>	Allow TCP syn packets with data to pass.	<i>drop</i>	Drop TCP syn packets with data.	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.		
Option	Description										
<i>allow</i>	Allow TCP syn packets with data to pass.										
<i>drop</i>	Drop TCP syn packets with data.										
<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.										
tcp-syn-fin	TCP SYN flood SYN/FIN flag set anomalies.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	allow	Allow TCP packets with syn_fin flag set to pass.	
	drop	Drop TCP packets with syn_fin flag set.	
	trap-to-host	Forward TCP packets with syn_fin flag set to FortiOS.	
tcp-winnuke	TCP WinNuke anomalies.	option	-
	Option	Description	
	allow	Allow TCP packets winnuke attack to pass.	
	drop	Drop TCP packets winnuke attack.	
	trap-to-host	Forward TCP packets winnuke attack to FortiOS.	
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-
	Option	Description	
	drop	Drop IPv4 invalid UDP checksum.	
	trap-to-host	Forward IPv4 invalid UDP checksum to main CPU for processing.	
udp-land	UDP land anomalies.	option	-
	Option	Description	
	allow	Allow UDP land attack to pass.	
	drop	Drop UDP land attack.	
	trap-to-host	Forward UDP land attack to FortiOS.	

config hpe

Parameter	Description	Type	Size				
arp-max	Maximum ARP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000				
enable-shaper	Enable/Disable NPU Host Protection Engine (HPE) for packet type shaper.	option	-				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NPU HPE shaping based on packet type.</td></tr></table>			Option	Description	<i>disable</i>	Disable NPU HPE shaping based on packet type.
Option	Description						
<i>disable</i>	Disable NPU HPE shaping based on packet type.						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable NPU HPE shaping based on packet type.	
esp-max	Maximum ESP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
icmp-max	Maximum ICMP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
ip-frag-max	Maximum fragmented IP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
ip-others-max	Maximum IP packet rate for other packets (packet types that cannot be set with other options) (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
pri-type-max	Maximum overflow rate of priority type traffic(1K - 1G pps, default = 200K pps). Includes L2: HA, 802.3ad LACP, heartbeats. L3: OSPF. L4_TCP: BGP. L4_UDP: IKE, SLBC, BFD.	integer	Minimum value: 1000 Maximum value: 1000000000
sctp-max	Maximum SCTP packet rate (1K - 1G pps, default = 200K pps).	integer	Minimum value: 1000 Maximum value: 1000000000

Parameter	Description	Type	Size
tcp-max	Maximum TCP packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
tcpfin-rst-max	Maximum TCP carries FIN or RST flags packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
tcpsyn-ack-max	Maximum TCP carries SYN and ACK flags packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
tcpsyn-max	Maximum TCP SYN packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000
udp-max	Maximum UDP packet rate (1K - 1G pps, default = 600K pps).	integer	Minimum value: 1000 Maximum value: 1000000000

config system np6xlite



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 101E, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 61E, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 81E-POE, FortiGate 81E, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 61E.

Configure NP6XLITE attributes.

```
config system np6xlite
    Description: Configure NP6XLITE attributes.
    edit <name>
        set asicdos [disable|enable]
        set fastpath [disable|enable]
        config fp-anomaly
            Description: NP6XLITE IPv4 anomaly protection. trap-to-host forwards anomaly
sessions to the CPU.
            set icmp-csum-err [drop|trap-to-host]
            set icmp-frag [allow|drop|...]
            set icmp-land [allow|drop|...]
            set ipv4-csum-err [drop|trap-to-host]
            set ipv4-land [allow|drop|...]
            set ipv4-optlsrr [allow|drop|...]
            set ipv4-optrr [allow|drop|...]
            set ipv4-optsecurity [allow|drop|...]
            set ipv4-optssrr [allow|drop|...]
            set ipv4-optstream [allow|drop|...]
            set ipv4-opttimestamp [allow|drop|...]
            set ipv4-proto-err [allow|drop|...]
            set ipv4-unknopt [allow|drop|...]
            set ipv6-daddr-err [allow|drop|...]
            set ipv6-land [allow|drop|...]
```

```

        set ipv6-optendpid [allow|drop|...]
        set ipv6-opthomeaddr [allow|drop|...]
        set ipv6-optinvld [allow|drop|...]
        set ipv6-optjumbo [allow|drop|...]
        set ipv6-optnsap [allow|drop|...]
        set ipv6-optralert [allow|drop|...]
        set ipv6-opttunnel [allow|drop|...]
        set ipv6-proto-err [allow|drop|...]
        set ipv6-saddr-err [allow|drop|...]
        set ipv6-unknopt [allow|drop|...]
        set tcp-csum-err [drop|trap-to-host]
        set tcp-fin-noack [allow|drop|...]
        set tcp-fin-only [allow|drop|...]
        set tcp-land [allow|drop|...]
        set tcp-no-flag [allow|drop|...]
        set tcp-syn-data [allow|drop|...]
        set tcp-syn-fin [allow|drop|...]
        set tcp-winnuke [allow|drop|...]
        set udp-csum-err [drop|trap-to-host]
        set udp-land [allow|drop|...]
    end
    set garbage-session-collector [disable|enable]
    config hpe
        Description: HPE configuration.
        set arp-max {integer}
        set enable-shaper [disable|enable]
        set esp-max {integer}
        set icmp-max {integer}
        set ip-frag-max {integer}
        set ip-others-max {integer}
        set l2-others-max {integer}
        set sctp-max {integer}
        set tcp-max {integer}
        set tcpsyn-max {integer}
        set udp-max {integer}
    end
    set ipsec-inner-fragment [disable|enable]
    set per-session-accounting [disable|traffic-log-only|...]
    set session-collector-interval {integer}
    set session-timeout-fixed [disable|enable]
    set session-timeout-interval {integer}
    set session-timeout-random-range {integer}
next
end

```

config system np6xlite

Parameter	Description	Type	Size
asicdos *	Enable/disable NP6XLITE DoS offloading.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable NP6XLITE DoS offloading (DoS done by host).	
	<i>enable</i>	Enable NP6XLITE DoS offloading (DoS done by asic).	
fastpath	Enable/disable NP4 or NP6XLITE offloading (also called fast path).	option	-
	Option	Description	
	<i>disable</i>	Disable NP4 or NP6XLITE offloading (fast path).	
	<i>enable</i>	Enable NP4 or NP6XLITE offloading (fast path).	
garbage-session-collector	Enable/disable garbage session collector.	option	-
	Option	Description	
	<i>disable</i>	Disable garbage session collector.	
	<i>enable</i>	Enable garbage session collector.	
ipsec-inner-fragment	Enable/disable NP6XLite IPsec fragmentation type: inner.	option	-
	Option	Description	
	<i>disable</i>	NP6XLite ipsec fragmentation type: outer.	
	<i>enable</i>	Enable NP6XLite ipsec fragmentation type: inner.	
name	Device Name.	string	Maximum length: 31
per-session-accounting	Enable/disable per-session accounting.	option	-
	Option	Description	
	<i>disable</i>	Disable per-session accounting.	
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.	
	<i>enable</i>	Per-session accounting for all sessions.	
session-collector-interval	Set garbage session collection cleanup interval (1 - 100 sec, default 64).	integer	Minimum value: 1 Maximum value: 100

Parameter	Description	Type	Size
session-timeout-fixed	Enable/disable fixed timeout interval mode.	option	-
	Option	Description	
	<i>disable</i>	Disable NPU session timeout at fixed interval.	
	<i>enable</i>	Enable NPU session timeout at fixed interval.	
session-timeout-interval	Set session timeout interval (0 - 1000 sec, default 40 sec).	integer	Minimum value: 0 Maximum value: 1000
session-timeout-random-range	Set the randomization range (0 - 1000 sec, default 8 sec).	integer	Minimum value: 0 Maximum value: 1000

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid ICMP checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.	
icmp-frag	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.	
	<i>drop</i>	Drop L3 fragment packet with L4 protocol as ICMP attack.	
	<i>trap-to-host</i>	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.	
icmp-land	ICMP land anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow ICMP land attack to pass.	
	<i>drop</i>	Drop ICMP land attack.	
	<i>trap-to-host</i>	Forward ICMP land attack to FortiOS.	

Parameter	Description	Type	Size								
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid IP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid IP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid IP checksum.	trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.				
Option	Description										
drop	Drop IPv4 invalid IP checksum.										
trap-to-host	Forward IPv4 invalid IP checksum to main CPU for processing.										
ipv4-land	Land anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 land attack to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 land attack.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 land attack to pass.	drop	Drop IPv4 land attack.	trap-to-host	Forward IPv4 land attack to FortiOS.		
Option	Description										
allow	Allow IPv4 land attack to pass.										
drop	Drop IPv4 land attack.										
trap-to-host	Forward IPv4 land attack to FortiOS.										
ipv4-optlsrr	Loose source record route option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with loose source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with loose source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with loose source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with loose source record route option to pass.	drop	Drop IPv4 with loose source record route option.	trap-to-host	Forward IPv4 with loose source record route option to FortiOS.		
Option	Description										
allow	Allow IPv4 with loose source record route option to pass.										
drop	Drop IPv4 with loose source record route option.										
trap-to-host	Forward IPv4 with loose source record route option to FortiOS.										
ipv4-optrr	Record route option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with record route option to pass.	drop	Drop IPv4 with record route option.	trap-to-host	Forward IPv4 with record route option to FortiOS.		
Option	Description										
allow	Allow IPv4 with record route option to pass.										
drop	Drop IPv4 with record route option.										
trap-to-host	Forward IPv4 with record route option to FortiOS.										
ipv4-optsecurity	Security option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with security option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with security option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with security option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with security option to pass.	drop	Drop IPv4 with security option.	trap-to-host	Forward IPv4 with security option to FortiOS.		
Option	Description										
allow	Allow IPv4 with security option to pass.										
drop	Drop IPv4 with security option.										
trap-to-host	Forward IPv4 with security option to FortiOS.										
ipv4-optssrr	Strict source record route option anomalies.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with strict source record route option to pass.</td></tr></table>	Option	Description	allow	Allow IPv4 with strict source record route option to pass.						
Option	Description										
allow	Allow IPv4 with strict source record route option to pass.										

Parameter	Description	Type	Size
	Option	Description	
	<i>drop</i>	Drop IPv4 with strict source record route option.	
	<i>trap-to-host</i>	Forward IPv4 with strict source record route option to FortiOS.	
ipv4-optstream	Stream option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with stream option to pass.	
	<i>drop</i>	Drop IPv4 with stream option.	
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.	
ipv4-opttimestamp	Timestamp option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with timestamp option to pass.	
	<i>drop</i>	Drop IPv4 with timestamp option.	
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.	
ipv4-proto-err	Invalid layer 4 protocol anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 invalid L4 protocol to pass.	
	<i>drop</i>	Drop IPv4 invalid L4 protocol.	
	<i>trap-to-host</i>	Forward IPv4 invalid L4 protocol to FortiOS.	
ipv4-unknpt	Unknown option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv4 with unknown options to pass.	
	<i>drop</i>	Drop IPv4 with unknown options.	
	<i>trap-to-host</i>	Forward IPv4 with unknown options to FortiOS.	
ipv6-daddr-err	Destination address as unspecified or loopback address anomalies.	option	-

Parameter	Description	Type	Size
	Option	Description	
	allow	Allow IPv6 with destination address as unspecified or loopback address to pass.	
	drop	Drop IPv6 with destination address as unspecified or loopback address.	
	trap-to-host	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.	
ipv6-land	Land anomalies.	option	-
	Option	Description	
	allow	Allow IPv6 land attack to pass.	
	drop	Drop IPv6 land attack.	
	trap-to-host	Forward IPv6 land attack to FortiOS.	
ipv6-optendpid	End point identification anomalies.	option	-
	Option	Description	
	allow	Allow IPv6 with end point identification option to pass.	
	drop	Drop IPv6 with end point identification option.	
	trap-to-host	Forward IPv6 with end point identification option to FortiOS.	
ipv6-opthomeaddr	Home address option anomalies.	option	-
	Option	Description	
	allow	Allow IPv6 with home address option to pass.	
	drop	Drop IPv6 with home address option.	
	trap-to-host	Forward IPv6 with home address option to FortiOS.	
ipv6-optinvld	Invalid option anomalies.Invalid option anomalies.	option	-
	Option	Description	
	allow	Allow IPv6 with invalid option to pass.	
	drop	Drop IPv6 with invalid option.	
	trap-to-host	Forward IPv6 with invalid option to FortiOS.	
ipv6-optjumbo	Jumbo options anomalies.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>allow</i>	Allow IPv6 with jumbo option to pass.	
	<i>drop</i>	Drop IPv6 with jumbo option.	
	<i>trap-to-host</i>	Forward IPv6 with jumbo option to FortiOS.	
ipv6-optnsap	Network service access point address option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 with network service access point address option to pass.	
	<i>drop</i>	Drop IPv6 with network service access point address option.	
	<i>trap-to-host</i>	Forward IPv6 with network service access point address option to FortiOS.	
ipv6-optralert	Router alert option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 with router alert option to pass.	
	<i>drop</i>	Drop IPv6 with router alert option.	
	<i>trap-to-host</i>	Forward IPv6 with router alert option to FortiOS.	
ipv6-opttunnel	Tunnel encapsulation limit option anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 with tunnel encapsulation limit to pass.	
	<i>drop</i>	Drop IPv6 with tunnel encapsulation limit.	
	<i>trap-to-host</i>	Forward IPv6 with tunnel encapsulation limit to FortiOS.	
ipv6-proto-err	Layer 4 invalid protocol anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 L4 invalid protocol to pass.	
	<i>drop</i>	Drop IPv6 L4 invalid protocol.	
	<i>trap-to-host</i>	Forward IPv6 L4 invalid protocol to FortiOS.	
ipv6-saddr-err	Source address as multicast anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow IPv6 with source address as multicast to pass.	

Parameter	Description	Type	Size
	Option	Description	
	drop	Drop IPv6 with source address as multicast.	
	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.	
ipv6-unknopt	Unknown option anomalies.	option	-
	Option	Description	
	allow	Allow IPv6 with unknown options to pass.	
	drop	Drop IPv6 with unknown options.	
	trap-to-host	Forward IPv6 with unknown options to FortiOS.	
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-
	Option	Description	
	drop	Drop IPv4 invalid TCP checksum.	
	trap-to-host	Forward IPv4 invalid TCP checksum to main CPU for processing.	
tcp-fin-noack	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-
	Option	Description	
	allow	Allow TCP packets with FIN flag set without ack setting to pass.	
	drop	Drop TCP packets with FIN flag set without ack setting.	
	trap-to-host	Forward TCP packets with FIN flag set without ack setting to FortiOS.	
tcp-fin-only	TCP SYN flood with only FIN flag set anomalies.	option	-
	Option	Description	
	allow	Allow TCP packets with FIN flag set only to pass.	
	drop	Drop TCP packets with FIN flag set only.	
	trap-to-host	Forward TCP packets with FIN flag set only to FortiOS.	
tcp-land	TCP land anomalies.	option	-
	Option	Description	
	allow	Allow TCP land attack to pass.	
	drop	Drop TCP land attack.	
	trap-to-host	Forward TCP land attack to FortiOS.	

Parameter	Description	Type	Size
tcp-no-flag	TCP SYN flood with no flag set anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow TCP packets without flag set to pass.	
	<i>drop</i>	Drop TCP packets without flag set.	
	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.	
tcp-syn-data	TCP SYN flood packets with data anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow TCP syn packets with data to pass.	
	<i>drop</i>	Drop TCP syn packets with data.	
	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.	
tcp-syn-fin	TCP SYN flood SYN/FIN flag set anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow TCP packets with syn_fin flag set to pass.	
	<i>drop</i>	Drop TCP packets with syn_fin flag set.	
	<i>trap-to-host</i>	Forward TCP packets with syn_fin flag set to FortiOS.	
tcp-winnuke	TCP WinNuke anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow TCP packets winnuke attack to pass.	
	<i>drop</i>	Drop TCP packets winnuke attack.	
	<i>trap-to-host</i>	Forward TCP packets winnuke attack to FortiOS.	
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP checksum to main CPU for processing.	
udp-land	UDP land anomalies.	option	-
	Option	Description	
	<i>allow</i>	Allow UDP land attack to pass.	

Parameter	Description	Type	Size
	Option	Description	
	<i>drop</i>	Drop UDP land attack.	
	<i>trap-to-host</i>	Forward UDP land attack to FortiOS.	

config hpe

Parameter	Description	Type	Size
arp-max	Maximum ARP packet rate (10K - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
enable-shaper	Enable/Disable NPU host protection engine (HPE) shaper.	option	-
	Option	Description	
	<i>disable</i>	Disable NPU HPE shaping based on packet type.	
	<i>enable</i>	Enable NPU HPE shaping based on packet type.	
esp-max	Maximum ESP packet rate (10K - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
icmp-max	Maximum ICMP packet rate (10K - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
ip-frag-max	Maximum fragmented IP packet rate (10K - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
ip-others-max	Maximum IP packet rate for other packets (packet types that cannot be set with other options) (10G - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000

Parameter	Description	Type	Size
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets (10K - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
sctp-max	Maximum SCTP packet rate (10K - 4G pps, default = 1M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
tcp-max	Maximum TCP packet rate (10K - 4G pps, default = 5M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
tcpsyn-max	Maximum TCP SYN packet rate (10K - 4G pps, default = 5M pps).	integer	Minimum value: 10000 Maximum value: 4000000000
udp-max	Maximum UDP packet rate (10K - 4G pps, default = 5M pps).	integer	Minimum value: 10000 Maximum value: 4000000000

config system npu



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100D, FortiGate 140D-POE, FortiGate 140D, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E.

Configure NPU attributes.

config system npu

Description: Configure NPU attributes.

set capwap-offload [enable|disable]

set dedicated-management-cpu [enable|disable]

set fastpath [disable|enable]

config fp-anomaly

Description: NP6Lite anomaly protection (packet drop or send trap to host).

set esp-minlen-err [drop|trap-to-host]

set icmp-csum-err [drop|trap-to-host]

set icmp-minlen-err [drop|trap-to-host]

set ipv4-csum-err [drop|trap-to-host]

set ipv4-ihl-err [drop|trap-to-host]

set ipv4-len-err [drop|trap-to-host]

set ipv4-opt-err [drop|trap-to-host]

set ipv4-ttlzero-err [drop|trap-to-host]

set ipv4-ver-err [drop|trap-to-host]

set ipv6-exthdr-len-err [drop|trap-to-host]

set ipv6-exthdr-order-err [drop|trap-to-host]

set ipv6-ihl-err [drop|trap-to-host]

set ipv6-plen-zero [drop|trap-to-host]

set ipv6-ver-err [drop|trap-to-host]

set tcp-csum-err [drop|trap-to-host]

```

    set tcp-hlen-err [drop|trap-to-host]
    set tcp-plen-err [drop|trap-to-host]
    set udp-csum-err [drop|trap-to-host]
    set udp-hlen-err [drop|trap-to-host]
    set udp-len-err [drop|trap-to-host]
    set udp-plen-err [drop|trap-to-host]
    set udplite-cover-err [drop|trap-to-host]
    set udplite-csum-err [drop|trap-to-host]
    set unknproto-minlen-err [drop|trap-to-host]
end
set gtp-enhanced-cpu-range [0|1|...]
set gtp-enhanced-mode [enable|disable]
set host-shortcut-mode [bi-directional|host-shortcut]
set htx-gtse-quota [100Mbps|200Mbps|...]
set iph-rsvd-re-cksum [enable|disable]
set ipsec-dec-subengine-mask {user}
set ipsec-enc-subengine-mask {user}
set ipsec-inbound-cache [enable|disable]
set ipsec-mtu-override [disable|enable]
set ipsec-over-vlink [enable|disable]
config isf-np-queues
    Description: Configure queues of switch port connected to NP6 XAUI on ingress path.
    set cos0 {string}
    set cos1 {string}
    set cos2 {string}
    set cos3 {string}
    set cos4 {string}
    set cos5 {string}
    set cos6 {string}
    set cos7 {string}
end
set lag-out-port-select [disable|enable]
set mcast-session-accounting [tpe-based|session-based|...]
set np6-cps-optimization-mode [enable|disable]
set per-session-accounting [disable|traffic-log-only|...]
config port-cpu-map
    Description: Configure NPU interface to CPU core mapping.
    edit <interface>
        set cpu-core {string}
    next
end
config port-npu-map
    Description: Configure port to NPU group mapping.
    edit <interface>
        set npu-group-index {integer}
    next
end
config priority-protocol
    Description: Configure NPU priority protocol.
    set bfd [enable|disable]
    set bgp [enable|disable]
    set slbc [enable|disable]
end
set qos-mode [disable|priority|...]
set rdp-offload [enable|disable]
set recover-np6-link [enable|disable]

```

```

set sse-backpressure [enable|disable]
set strip-clear-text-padding [enable|disable]
set strip-esp-padding [enable|disable]
set sw-np-bandwidth [0G|2G|...]
set switch-np-hash [src-ip|dst-ip|...]
set uesp-offload [enable|disable]
end

```

config system npu

Parameter	Description	Type	Size								
capwap-offload *	Enable/disable offloading managed FortiAP and FortiLink CAPWAP sessions.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable CAPWAP offload.</td></tr><tr><td>disable</td><td>Disable CAPWAP offload.</td></tr></table>	Option	Description	enable	Enable CAPWAP offload.	disable	Disable CAPWAP offload.				
Option	Description										
enable	Enable CAPWAP offload.										
disable	Disable CAPWAP offload.										
dedicated-management-cpu *	Enable to dedicate one CPU for GUI and CLI connections when NPs are busy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dedication of CPU #0 for management tasks.</td></tr><tr><td>disable</td><td>Disable dedication of CPU #0 for management tasks.</td></tr></table>	Option	Description	enable	Enable dedication of CPU #0 for management tasks.	disable	Disable dedication of CPU #0 for management tasks.				
Option	Description										
enable	Enable dedication of CPU #0 for management tasks.										
disable	Disable dedication of CPU #0 for management tasks.										
fastpath *	Enable/disable NP6 offloading (also called fast path).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP6 offloading (fast path).</td></tr><tr><td>enable</td><td>Enable NP6 offloading (fast path).</td></tr></table>	Option	Description	disable	Disable NP6 offloading (fast path).	enable	Enable NP6 offloading (fast path).				
Option	Description										
disable	Disable NP6 offloading (fast path).										
enable	Enable NP6 offloading (fast path).										
gtp-enhanced-cpu-range *	GTP enhanced CPU range option.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>Inspect GTPU packets by all CPUs.</td></tr><tr><td>1</td><td>Inspect GTPU packets by Master CPUs.</td></tr><tr><td>2</td><td>Inspect GTPU packets by Slave CPUs.</td></tr></table>	Option	Description	0	Inspect GTPU packets by all CPUs.	1	Inspect GTPU packets by Master CPUs.	2	Inspect GTPU packets by Slave CPUs.		
Option	Description										
0	Inspect GTPU packets by all CPUs.										
1	Inspect GTPU packets by Master CPUs.										
2	Inspect GTPU packets by Slave CPUs.										
gtp-enhanced-mode *	Enable/disable GTP enhanced mode.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable GTP enhanced mode.	
	<i>disable</i>	Disable GTP enhanced mode.	
host-shortcut-mode *	Set np6 host shortcut mode.	option	-
	Option	Description	
	<i>bi-directional</i>	Offload TCP and IP Tunnel sessions in both directions between 10G and 1G interfaces (normal operation).	
	<i>host-shortcut</i>	Only offload TCP and IP Tunnel sessions received by 1G interfaces. Select if packets are dropped for offloaded traffic between 10G to 1G interfaces.	
htx-gtse-quota *	Configure HTX GTSE quota.	option	-
	Option	Description	
	<i>100Mbps</i>	100Mbps.	
	<i>200Mbps</i>	200Mbps.	
	<i>300Mbps</i>	300Mbps.	
	<i>400Mbps</i>	400Mbps.	
	<i>500Mbps</i>	500Mbps.	
	<i>600Mbps</i>	600Mbps.	
	<i>700Mbps</i>	700Mbps.	
	<i>800Mbps</i>	800Mbps.	
	<i>900Mbps</i>	900Mbps.	
	<i>1Gbps</i>	1Gbps.	
	<i>2Gbps</i>	2Gbps.	
	<i>4Gbps</i>	4Gbps.	
	<i>8Gbps</i>	8Gbps.	
	<i>10Gbps</i>	10Gbps.	
iph-rsvd-recksum *	Enable/disable IP checksum re-calculation for packets with iph.reserved bit set.	option	-
	Option	Description	
	<i>enable</i>	Enable IP checksum re-calculation for packets with iph.reserved bit set.	

Parameter	Description	Type	Size

Option		Description
	<i>disable</i>	Disable IP checksum re-calculation for packets with iph.reserved bit set.

ipsec-dec-subengine-mask *	IPsec decryption subengine mask (0x1 - 0xff, default 0xff).	user	Not Specified
ipsec-enc-subengine-mask *	IPsec encryption subengine mask (0x1 - 0xff, default 0xff).	user	Not Specified
ipsec-inbound-cache *	Enable/disable IPsec inbound cache for anti-replay.	option	-

Option		Description
	<i>enable</i>	Enable inbound cache always.
	<i>disable</i>	Disable inbound cache when IPsec anti-replay is on.

ipsec-mtu-override *	Enable/disable NP6 IPsec MTU override.	option	-

Option		Description
	<i>disable</i>	Disable NP6 IPsec MTU override.
	<i>enable</i>	Enable NP6 IPsec MTU override.

ipsec-over-vlink *	Enable/disable IPSEC over vlink.	option	-

Option		Description
	<i>enable</i>	Enable IPSEC over vlink.
	<i>disable</i>	Disable IPSEC over vlink.

lag-out-port-select *	Enable/disable LAG outgoing port selection based on incoming traffic port.	option	-

Option		Description
	<i>disable</i>	Disable LAG outgoing port selection based on incoming traffic port.
	<i>enable</i>	Enable LAG outgoing port selection based on incoming traffic port.

mcast-session-accounting *	Enable/disable traffic accounting for each multicast session through TAE counter.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>tpe-based</i>	Enable TPE-based multicast session accounting.	
	<i>session-based</i>	Enable session-based multicast session accounting.	
	<i>disable</i>	Disable multicast session accounting.	
np6-cps-optimization-mode *	Enable/disable NP6 connection per second (CPS) optimization mode.	option	-
	Option	Description	
	<i>enable</i>	Enable NP6 connection per second (CPS) optimization mode.	
	<i>disable</i>	Disable NP6 connection per second (CPS) optimization mode.	
per-session-accounting *	Enable/disable per-session accounting.	option	-
	Option	Description	
	<i>disable</i>	Disable per-session accounting.	
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.	
	<i>enable</i>	Per-session accounting for all sessions.	
qos-mode *	QoS mode on switch and NP.	option	-
	Option	Description	
	<i>disable</i>	Disable QoS on switch and NP.	
	<i>priority</i>	Priority based.	
	<i>round-robin</i>	Round Robin Scheduler.	
rdp-offload *	Enable/disable rdp offload.	option	-
	Option	Description	
	<i>enable</i>	Enable reliable datagram protocol traffic offload.	
	<i>disable</i>	Disable reliable datagram protocol traffic offload.	
recover-np6-link *	Enable/disable internal link failure check and recovery after boot up.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable internal link failure check and recovery after boot up.	
	<i>disable</i>	Disable internal link failure check and recovery after boot up.	
sse-backpressure *	Enable/disable sse backpressure.	option	-
	Option	Description	
	<i>enable</i>	Enable sse backpressure.	
	<i>disable</i>	Disable sse backpressure.	
strip-clear-text-padding *	Enable/disable stripping clear text padding.	option	-
	Option	Description	
	<i>enable</i>	Enable stripping clear text padding.	
	<i>disable</i>	Disable stripping clear text padding.	
strip-esp-padding *	Enable/disable stripping ESP padding.	option	-
	Option	Description	
	<i>enable</i>	Enable stripping ESP padding.	
	<i>disable</i>	Disable stripping ESP padding.	
sw-np-bandwidth *	Bandwidth from switch to NP.	option	-
	Option	Description	
	<i>0G</i>	Default value. No bandwidth control.	
	<i>2G</i>	2Gbps.	
	<i>4G</i>	4Gbps.	
	<i>5G</i>	5Gbps.	
	<i>6G</i>	6Gbps.	
switch-np-hash *	Switch-NP trunk port selection Criteria.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>src-ip</i>	Source IP address.	
	<i>dst-ip</i>	Destination IP address.	
	<i>src-dst-ip</i>	Source+dest IP address.	
uesp-offload *	Enable/disable UDP-encapsulated ESP offload (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable UDP-encapsulated ESP traffic offload.	
	<i>disable</i>	Disable UDP-encapsulated ESP traffic offload.	

* This parameter may not exist in some models.

config fp-anomaly

Parameter	Description	Type	Size
esp-minlen-err	Invalid IPv4 ESP short packet anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid ESP short packet.	
	<i>trap-to-host</i>	Forward IPv4 invalid ESP short packet to main CPU for processing.	
icmp-csum-err	Invalid IPv4 ICMP packet checksum anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid ICMP checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid ICMP checksum to main CPU for processing.	
icmp-minlen-err	Invalid IPv4 ICMP short packet anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid ICMP short packet.	
	<i>trap-to-host</i>	Forward IPv4 invalid ICMP short packet to main CPU for processing.	
ipv4-csum-err	Invalid IPv4 packet checksum anomalies.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid L3 checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid L3 checksum to main CPU for processing.	
ipv4-ihl-err	Invalid IPv4 header length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid header length.	
	<i>trap-to-host</i>	Forward IPv4 invalid header length to main CPU for processing.	
ipv4-len-err	Invalid IPv4 packet length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid packet length.	
	<i>trap-to-host</i>	Forward IPv4 invalid packet length to main CPU for processing.	
ipv4-opt-err	Invalid IPv4 option parsing anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid option parsing.	
	<i>trap-to-host</i>	Forward IPv4 invalid option parsing to main CPU for processing.	
ipv4-ttlzero-err	Invalid IPv4 TTL field zero anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid TTL field zero.	
	<i>trap-to-host</i>	Forward IPv4 invalid TTL field zero to main CPU for processing.	
ipv4-ver-err	Invalid IPv4 header version anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid header version.	
	<i>trap-to-host</i>	Forward IPv4 invalid header version to main CPU for processing.	
ipv6-exthdr-len-err	Invalid IPv6 packet chain extension header total length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv6 with invalid packet chain extension header total length.	

Parameter	Description	Type	Size
	Option	Description	
	<i>trap-to-host</i>	Forward IPv6 with invalid packet chain extension header total length to FortiOS.	
ipv6-exthdr-order-err	Invalid IPv6 packet extension header ordering anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv6 with invalid packet extension header ordering.	
	<i>trap-to-host</i>	Forward IPv6 with invalid packet extension header ordering to FortiOS.	
ipv6-ihl-err	Invalid IPv6 packet length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv6 with invalid packet length.	
	<i>trap-to-host</i>	Forward IPv6 with invalid packet length to FortiOS.	
ipv6-plen-zero	Invalid IPv6 packet payload length zero anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv6 with invalid packet payload length zero.	
	<i>trap-to-host</i>	Forward IPv6 with invalid packet payload length zero to FortiOS.	
ipv6-ver-err	Invalid IPv6 packet version anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv6 with invalid packet version.	
	<i>trap-to-host</i>	Forward IPv6 with invalid packet version to FortiOS.	
tcp-csum-err	Invalid IPv4 TCP packet checksum anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid TCP packet checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet checksum to main CPU for processing.	
tcp-hlen-err	Invalid IPv4 TCP header length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid TCP packet header length.	
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet header length to main CPU for processing.	

Parameter	Description	Type	Size
tcp-plen-err	Invalid IPv4 TCP packet length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid TCP packet length.	
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet length to main CPU for processing.	
udp-csum-err	Invalid IPv4 UDP packet checksum anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP packet checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet checksum to main CPU for processing.	
udp-hlen-err	Invalid IPv4 UDP packet header length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP header length.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP header length to main CPU for processing.	
udp-len-err	Invalid IPv4 UDP packet length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP packet length.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet length to main CPU for processing.	
udp-plen-err	Invalid IPv4 UDP packet minimum length anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP packet minimum length.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet minimum length to main CPU for processing.	
udplite-cover-err	Invalid IPv4 UDP-Lite packet coverage anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP-Lite packet coverage.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.	
udplite-csum-err	Invalid IPv4 UDP-Lite packet checksum anomalies.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid UDP-Lite packet checksum.	
	<i>trap-to-host</i>	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.	
unknproto-minlen-err	Invalid IPv4 L4 unknown protocol short packet anomalies.	option	-
	Option	Description	
	<i>drop</i>	Drop IPv4 invalid L4 unknown protocol short packet.	
	<i>trap-to-host</i>	Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.	

config isf-np-queues

Parameter	Description	Type	Size
cos0	CoS profile name for CoS 0.	string	Maximum length: 35
cos1	CoS profile name for CoS 1.	string	Maximum length: 35
cos2	CoS profile name for CoS 2.	string	Maximum length: 35
cos3	CoS profile name for CoS 3.	string	Maximum length: 35
cos4	CoS profile name for CoS 4.	string	Maximum length: 35
cos5	CoS profile name for CoS 5.	string	Maximum length: 35
cos6	CoS profile name for CoS 6.	string	Maximum length: 35
cos7	CoS profile name for CoS 7.	string	Maximum length: 35

config port-cpu-map

Parameter	Description	Type	Size
cpu-core	The CPU core to map to an interface.	string	Maximum length: 31
interface	The interface to map to a CPU core.	string	Maximum length: 15

config port-npu-map

Parameter	Description	Type	Size
interface	Set npu interface port to NPU group map.	string	Maximum length: 15
npu-group-index	Mapping NPU group index.	integer	Minimum value: 0 Maximum value: 4294967295

config priority-protocol

Parameter	Description	Type	Size						
bfd	Enable/disable NPU BFD priority protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU BFD priority protocol.</td></tr><tr><td><i>disable</i></td><td>Disable NPU BFD priority protocol.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU BFD priority protocol.	<i>disable</i>	Disable NPU BFD priority protocol.		
Option	Description								
<i>enable</i>	Enable NPU BFD priority protocol.								
<i>disable</i>	Disable NPU BFD priority protocol.								
bgp	Enable/disable NPU BGP priority protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU BGP priority protocol.</td></tr><tr><td><i>disable</i></td><td>Disable NPU BGP priority protocol.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU BGP priority protocol.	<i>disable</i>	Disable NPU BGP priority protocol.		
Option	Description								
<i>enable</i>	Enable NPU BGP priority protocol.								
<i>disable</i>	Disable NPU BGP priority protocol.								
slbc	Enable/disable NPU SLBC priority protocol.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU SLBC priority protocol.</td></tr><tr><td><i>disable</i></td><td>Disable NPU SLBC priority protocol.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU SLBC priority protocol.	<i>disable</i>	Disable NPU SLBC priority protocol.		
Option	Description								
<i>enable</i>	Enable NPU SLBC priority protocol.								
<i>disable</i>	Disable NPU SLBC priority protocol.								

config system ntp

Configure system NTP information.

```
config system ntp
  Description: Configure system NTP information.
  set authentication [enable|disable]
  set interface <interface-name1>, <interface-name2>, ...
  set key {password}
  set key-id {integer}
  set key-type [MD5|SHA1]
  config ntpserver
```

Description: Configure the FortiGate to connect to any available third-party NTP server.

```
edit <id>
    set authentication [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set key {password}
    set key-id {integer}
    set ntpv3 [enable|disable]
    set server {string}
next
end
set ntpsync [enable|disable]
set server-mode [enable|disable]
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set syncinterval {integer}
set type [fortiguard|custom]
end
```

config system ntp

Parameter	Description	Type	Size						
authentication	Enable/disable authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication.</td></tr><tr><td><i>disable</i></td><td>Disable authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.		
	Option	Description							
	<i>enable</i>	Enable authentication.							
<i>disable</i>	Disable authentication.								
interface <interface-name>	FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79						
key	Key for authentication.	password	Not Specified						
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295						
key-type	Key type for authentication (MD5, SHA1).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>MD5</i></td><td>Use MD5 to authenticate the message.</td></tr><tr><td><i>SHA1</i></td><td>Use SHA1 to authenticate the message.</td></tr></table>	Option	Description	<i>MD5</i>	Use MD5 to authenticate the message.	<i>SHA1</i>	Use SHA1 to authenticate the message.		
	Option	Description							
	<i>MD5</i>	Use MD5 to authenticate the message.							
<i>SHA1</i>	Use SHA1 to authenticate the message.								

Parameter	Description	Type	Size						
ntpsync	Enable/disable setting the FortiGate system time by synchronizing with an NTP Server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with NTP Server.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with NTP Server.</td></tr></table>	Option	Description	<i>enable</i>	Enable synchronization with NTP Server.	<i>disable</i>	Disable synchronization with NTP Server.		
Option	Description								
<i>enable</i>	Enable synchronization with NTP Server.								
<i>disable</i>	Disable synchronization with NTP Server.								
server-mode	Enable/disable FortiGate NTP Server Mode. Your FortiGate becomes an NTP server for other devices on your network. The FortiGate relays NTP requests to its configured NTP server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGate NTP Server Mode.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGate NTP Server Mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGate NTP Server Mode.	<i>disable</i>	Disable FortiGate NTP Server Mode.		
Option	Description								
<i>enable</i>	Enable FortiGate NTP Server Mode.								
<i>disable</i>	Disable FortiGate NTP Server Mode.								
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified						
source-ip6	Source IPv6 address for communication to the NTP server.	ipv6-address	Not Specified						
syncinterval	NTP synchronization interval (1 - 1440 min).	integer	Minimum value: 1 Maximum value: 1440						
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Use the FortiGuard NTP server.</td></tr><tr><td><i>custom</i></td><td>Use any other available NTP server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Use the FortiGuard NTP server.	<i>custom</i>	Use any other available NTP server.		
Option	Description								
<i>fortiguard</i>	Use the FortiGuard NTP server.								
<i>custom</i>	Use any other available NTP server.								

config ntpserver

Parameter	Description	Type	Size						
authentication	Enable/disable MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr><tr><td><i>disable</i></td><td>Disable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.	<i>disable</i>	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.		
Option	Description								
<i>enable</i>	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.								
<i>disable</i>	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.								

Parameter	Description	Type	Size
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
key	Key for MD5(NTPv3)/SHA1(NTPv4) authentication.	password	Not Specified
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295
ntp3	Enable to use NTPv3 instead of NTPv4.	option	-
	Option	Description	
	<i>enable</i>	Enable NTPv3.	
	<i>disable</i>	Disable NTPv3 (use NTPv4).	
server	IP address or hostname of the NTP Server.	string	Maximum length: 63

config system object-tagging

Configure object tagging.

```
config system object-tagging
  Description: Configure object tagging.
  edit <category>
    set address [disable|mandatory|...]
    set color {integer}
    set device [disable|mandatory|...]
    set interface [disable|mandatory|...]
    set multiple [enable|disable]
    set tags <name1>, <name2>, ...
```

next
end

config system object-tagging

Parameter	Description	Type	Size
address	Address.	option	-
	Option	Description	
	<i>disable</i>	Disable.	
	<i>mandatory</i>	Mandatory.	
	<i>optional</i>	Optional.	
category	Tag Category.	string	Maximum length: 63
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32
device	Device.	option	-
	Option	Description	
	<i>disable</i>	Disable.	
	<i>mandatory</i>	Mandatory.	
	<i>optional</i>	Optional.	
interface	Interface.	option	-
	Option	Description	
	<i>disable</i>	Disable.	
	<i>mandatory</i>	Mandatory.	
	<i>optional</i>	Optional.	
multiple	Allow multiple tag selection.	option	-
	Option	Description	
	<i>enable</i>	Enable multi-tagging.	
	<i>disable</i>	Disable multi-tagging.	
tags <name>	Tags. Tag name.	string	Maximum length: 79

config system password-policy

Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.

```
config system password-policy
    Description: Configure password policy for locally defined administrator passwords and
    IPsec VPN pre-shared keys.
    set apply-to {option1}, {option2}, ...
    set change-4-characters [enable|disable]
    set expire-day {integer}
    set expire-status [enable|disable]
    set min-lower-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-upper-case-letter {integer}
    set minimum-length {integer}
    set reuse-password [enable|disable]
    set status [enable|disable]
end
```

config system 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	-						
<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>admin-password</i></td><td>Apply to administrator passwords.</td></tr><tr><td><i>ipsec-preshared-key</i></td><td>Apply to IPsec pre-shared keys.</td></tr></table>				Option	Description	<i>admin-password</i>	Apply to administrator passwords.	<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.
Option	Description								
<i>admin-password</i>	Apply to administrator passwords.								
<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.								
change-4-characters	Enable/disable changing at least 4 characters for a new password (This attribute overrides reuse-password if both are enabled).	option	-						
<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable requiring that at least 4 characters must be changed in a new password.</td></tr><tr><td><i>disable</i></td><td>No requirements for the number of characters to change in a new password. A new password can be the same as the old password.</td></tr></table>				Option	Description	<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.	<i>disable</i>	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.
Option	Description								
<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.								
<i>disable</i>	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-day	Number of days after which passwords expire (1 - 999 days, default = 90).	integer	Minimum value: 1 Maximum value: 999						

Parameter	Description	Type	Size						
expire-status	Enable/disable password expiration.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.		
	Option	Description							
	<i>enable</i>	Passwords expire after expire-day days.							
<i>disable</i>	Passwords do not expire.								
min-lower-case-letter	Minimum number of lowercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
min-number	Minimum number of numeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
min-upper-case-letter	Minimum number of uppercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128						
reuse-password	Enable/disable reusing of password (if both reuse-password and change-4-characters are enabled, change-4-characters overrides).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Administrators are allowed to reuse the same password.</td></tr><tr><td><i>disable</i></td><td>Administrators must create a new password.</td></tr></table>	Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.		
	Option	Description							
	<i>enable</i>	Administrators are allowed to reuse the same password.							
<i>disable</i>	Administrators must create a new password.								
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.		
	Option	Description							
	<i>enable</i>	Enable password policy.							
<i>disable</i>	Disable password policy.								

config system password-policy-guest-admin

Configure the password policy for guest administrators.

```
config system password-policy-guest-admin
  Description: Configure the password policy for guest administrators.
  set apply-to {option1}, {option2}, ...
  set change-4-characters [enable|disable]
  set expire-day {integer}
  set expire-status [enable|disable]
  set min-lower-case-letter {integer}
  set min-non-alphanumeric {integer}
  set min-number {integer}
  set min-upper-case-letter {integer}
  set minimum-length {integer}
  set reuse-password [enable|disable]
  set status [enable|disable]
end
```

config system password-policy-guest-admin

Parameter	Description	Type	Size						
apply-to	Guest administrator to which this password policy applies.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>guest-admin-password</i></td><td>Apply to guest administrator password.</td></tr></table>			Option	Description	<i>guest-admin-password</i>	Apply to guest administrator password.		
Option	Description								
<i>guest-admin-password</i>	Apply to guest administrator password.								
change-4-characters	Enable/disable changing at least 4 characters for a new password (This attribute overrides reuse-password if both are enabled).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable requiring that at least 4 characters must be changed in a new password.</td></tr><tr><td><i>disable</i></td><td>No requirements for the number of characters to change in a new password. A new password can be the same as the old password.</td></tr></table>			Option	Description	<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.	<i>disable</i>	No requirements for the number of characters to change in a new password. A new password can be the same as the old password.
Option	Description								
<i>enable</i>	Enable requiring that at least 4 characters must be changed in a new password.								
<i>disable</i>	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-day	Number of days after which passwords expire (1 - 999 days, default = 90).	integer	Minimum value: 1 Maximum value: 999						
expire-status	Enable/disable password expiration.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.		
	Option	Description							
	<i>enable</i>	Passwords expire after expire-day days.							
<i>disable</i>	Passwords do not expire.								
min-lower-case-letter	Minimum number of lowercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
min-number	Minimum number of numeric characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
min-upper-case-letter	Minimum number of uppercase characters in password (0 - 128, default = 0).	integer	Minimum value: 0 Maximum value: 128						
minimum-length	Minimum password length (8 - 128, default = 8).	integer	Minimum value: 8 Maximum value: 128						
reuse-password	Enable/disable reusing of password (if both reuse-password and change-4-characters are enabled, change-4-characters overrides).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Administrators are allowed to reuse the same password.</td></tr><tr><td><i>disable</i></td><td>Administrators must create a new password.</td></tr></table>	Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.		
	Option	Description							
	<i>enable</i>	Administrators are allowed to reuse the same password.							
<i>disable</i>	Administrators must create a new password.								
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.		
	Option	Description							
	<i>enable</i>	Enable password policy.							
<i>disable</i>	Disable password policy.								

config system physical-switch



This command is available for model(s): FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3800D, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate-VM64, FortiGateRugged 35D, FortiGateRugged 90D.

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	
	<i>enable</i>	Enable layer 2 ageing timer.	
	<i>disable</i>	Disable layer 2 ageing timer.	

Parameter	Description	Type	Size
age-val	Layer 2 table age timer Value.	integer	Minimum value: 0 Maximum value: 4294967295
name	Name.	string	Maximum length: 15

config system pppoe-interface

Configure the PPPoE interfaces.

```
config system pppoe-interface
    Description: Configure the PPPoE interfaces.
    edit <name>
        set ac-name {string}
        set auth-type [auto|pap|...]
        set device {string}
        set dial-on-demand [enable|disable]
        set disc-retry-timeout {integer}
        set idle-timeout {integer}
        set ipunnumbered {ipv4-address}
        set ipv6 [enable|disable]
        set lcp-echo-interval {integer}
        set lcp-max-echo-fails {integer}
        set padt-retry-timeout {integer}
        set password {password}
        set pppoe-unnumbered-negotiate [enable|disable]
        set service-name {string}
        set username {string}
    next
end
```

config system pppoe-interface

Parameter	Description	Type	Size
ac-name	PPPoE AC name.	string	Maximum length: 63
auth-type	PPP authentication type to use.	option	-
	Option	Description	
	<i>auto</i>	Automatically choose the authentication method.	
	<i>pap</i>	PAP authentication.	

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.		
	Option	Description									
	<i>chap</i>	CHAP authentication.									
	<i>mschapv1</i>	MS-CHAPv1 authentication.									
<i>mschapv2</i>	MS-CHAPv2 authentication.										
device	Name for the physical interface.	string	Maximum length: 15								
dial-on-demand	Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE interface.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dial on demand.</td></tr><tr><td><i>disable</i></td><td>Disable dial on demand.</td></tr></table>	Option	Description	<i>enable</i>	Enable dial on demand.	<i>disable</i>	Disable dial on demand.				
	Option	Description									
	<i>enable</i>	Enable dial on demand.									
<i>disable</i>	Disable dial on demand.										
disc-retry-timeout	PPPoE discovery init timeout value in (0-4294967295 sec).	integer	Minimum value: 0 Maximum value: 4294967295								
idle-timeout	PPPoE auto disconnect after idle timeout (0-4294967295 sec).	integer	Minimum value: 0 Maximum value: 4294967295								
ipunnumbered	PPPoE unnumbered IP.	ipv4-address	Not Specified								
ipv6	Enable/disable IPv6 Control Protocol (IPv6CP).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPv6CP.</td></tr><tr><td><i>disable</i></td><td>Disable IPv6CP.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPv6CP.	<i>disable</i>	Disable IPv6CP.				
	Option	Description									
	<i>enable</i>	Enable IPv6CP.									
<i>disable</i>	Disable IPv6CP.										
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								

Parameter	Description	Type	Size
name	Name of the PPPoE interface.	string	Maximum length: 15
padt-retry-timeout	PPPoE terminate timeout value in (0-4294967295 sec).	integer	Minimum value: 0 Maximum value: 4294967295
password	Enter the password.	password	Not Specified
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-
	Option	Description	
	enable	Enable PPPoE unnumbered negotiation.	
	disable	Disable PPPoE unnumbered negotiation.	
service-name	PPPoE service name.	string	Maximum length: 63
username	User name.	string	Maximum length: 64

config system probe-response

Configure system probe response.

```
config system probe-response
    Description: Configure system probe response.
    set http-probe-value {string}
    set mode [none|http-probe|...]
    set password {password}
    set port {integer}
    set security-mode [none|authentication]
    set timeout {integer}
    set ttl-mode [reinit|decrease|...]
end
```

config system probe-response

Parameter	Description	Type	Size
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024

Parameter	Description	Type	Size
mode	SLA response mode.	option	-
	Option	Description	
	<i>none</i>	Disable probe.	
	<i>http-probe</i>	HTTP probe.	
	<i>twamp</i>	Two way active measurement protocol.	
password	Twamp responder password in authentication mode	password	Not Specified
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535
security-mode	Twamp responder security mode.	option	-
	Option	Description	
	<i>none</i>	Unauthenticated mode.	
	<i>authentication</i>	Authenticated mode.	
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600
ttl-mode	Mode for TWAMP packet TTL modification.	option	-
	Option	Description	
	<i>reinit</i>	Reinitialize TTL.	
	<i>decrease</i>	Decrease TTL.	
	<i>retain</i>	Retain TTL.	

config system proxy-arp

Configure proxy-ARP.

```
config system proxy-arp
  Description: Configure proxy-ARP.
  edit <id>
    set end-ip {ipv4-address}
    set interface {string}
    set ip {ipv4-address}
  next
end
```

config system proxy-arp

Parameter	Description	Type	Size
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295
interface	Interface acting proxy-ARP.	string	Maximum length: 15
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified

config system ptp

Configure system PTP information.

```
config system ptp
  Description: Configure system PTP information.
  set delay-mechanism [E2E|P2P]
  set interface {string}
  set mode [multicast|hybrid]
  set request-interval {integer}
  set status [enable|disable]
end
```

config system ptp

Parameter	Description	Type	Size
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-
	Option	Description	
	<i>E2E</i>	End to end delay detection.	
	<i>P2P</i>	Peer to peer delay detection.	
interface	PTP slave will reply through this interface.	string	Maximum length: 15
mode	Multicast transmission or hybrid transmission.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>multicast</i>	Send PTP packets with multicast.	
	<i>hybrid</i>	Send PTP packets with unicast and multicast.	
request-interval	The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.	integer	Minimum value: 1 Maximum value: 6
status	Enable/disable setting the FortiGate system time by synchronizing with an PTP Server.	option	-
	Option	Description	
	<i>enable</i>	Enable synchronization with PTP Server.	
	<i>disable</i>	Disable synchronization with PTP Server.	

config system replacemsg admin

Replacement messages. Read-only.

```
config system replacemsg admin
    Description: Replacement messages. Read-only.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

config system replacemsg admin

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	

Parameter	Description	Type	Size
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg alertmail

Replacement messages. Read-only.

```

config system replacemsg alertmail
    Description: Replacement messages. Read-only.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end

```

config system replacemsg alertmail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	

Parameter	Description	Type	Size
	Option	Description	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg auth

Replacement messages. Read-only.

```
config system replacemsg auth
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg auth

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg device-detection-portal

Replacement messages. Read-only.

```
config system replacemsg device-detection-portal
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg device-detection-portal

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
		Option	Description
		<i>none</i>	No format type.
		<i>text</i>	Text format.
		<i>html</i>	HTML format.
header	Header flag.	option	-
		Option	Description
		<i>none</i>	No header type.
		<i>http</i>	HTTP
		<i>8bit</i>	8 bit.
msg-type	Message type.	string	Maximum length: 28

config system replacemsg fortiguard-wf

Replacement messages. Read-only.

```
config system replacemsg fortiguard-wf
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
```

```

        set header [none|http|...]
    next
end

```

config system replacemsg fortiguard-wf

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	none	No format type.	
	text	Text format.	
	html	HTML format.	
header	Header flag.	option	-
	Option	Description	
	none	No header type.	
	http	HTTP	
	8bit	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg ftp

Replacement messages. Read-only.

```

config system replacemsg ftp
    Description: Replacement messages. Read-only.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end

```

config system replacemsg ftp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg http

Replacement messages. Read-only.

```
config system replacemsg http
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg http

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg icap

Replacement messages. Read-only.

```
config system replacemsg icap
    Description: Replacement messages. Read-only.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

config system replacemsg icap

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	

Parameter	Description	Type	Size
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg mail

Replacement messages. Read-only.

```
config system replacemsg mail
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg mail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	

Parameter	Description	Type	Size
	Option	Description	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg nac-quar

Replacement messages. Read-only.

```
config system replacemsg nac-quar
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg nac-quar

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg nntp

Replacement messages. Read-only.

```
config system replacemsg nntp
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg nntp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
		Option	Description
		<i>none</i>	No format type.
		<i>text</i>	Text format.
		<i>html</i>	HTML format.
header	Header flag.	option	-
		Option	Description
		<i>none</i>	No header type.
		<i>http</i>	HTTP
		<i>8bit</i>	8 bit.
msg-type	Message type.	string	Maximum length: 28

config system replacemsg spam

Replacement messages. Read-only.

```
config system replacemsg spam
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
  next
end
```

```

        set header [none|http|...]
    next
end

```

config system replacemsg spam

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	none	No format type.	
	text	Text format.	
	html	HTML format.	
header	Header flag.	option	-
	Option	Description	
	none	No header type.	
	http	HTTP	
	8bit	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg sslvpn

Replacement messages. Read-only.

```

config system replacemsg sslvpn
    Description: Replacement messages. Read-only.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end

```


config system replacemsg sslvpn

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg traffic-quota

Replacement messages. Read-only.

```
config system replacemsg traffic-quota
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg traffic-quota

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg utm

Replacement messages. Read-only.

```
config system replacemsg utm
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg utm

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	

Parameter	Description	Type	Size
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg webproxy

Replacement messages. Read-only.

```
config system replacemsg webproxy
  Description: Replacement messages. Read-only.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

config system replacemsg webproxy

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	

Parameter	Description	Type	Size
	Option	Description	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config system replacemsg-group

Configure replacement message groups.

```
config system replacemsg-group
  Description: Configure replacement message groups.
  edit <name>
    config admin
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    config alertmail
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    config auth
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    set comment {var-string}
    config custom-message
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
      next
    end
    config device-detection-portal
      Description: Replacement message table entries.
      edit <msg-type>
```

```

        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config fortiguard-wf
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config ftp
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
set group-type [default|utm|...]
config http
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config icap
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config mail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config nac-quar
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
config nntp
    Description: Replacement message table entries.

```

```

        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config spam
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config sslvpn
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config traffic-quota
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config utm
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
    config webproxy
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set format [none|text|...]
            set header [none|http|...]
        next
    end
next
end

```

config system replacemsg-group

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
group-type	Group type.	option	-
	Option	Description	
	<i>default</i>	Per-vdom replacement messages.	
	<i>utm</i>	For use with UTM settings in firewall policies.	
	<i>auth</i>	For use with authentication pages in firewall policies.	
name	Group name.	string	Maximum length: 35

config admin

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config alertmail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config auth

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	

Parameter	Description	Type	Size
msg-type	Message type.	string	Maximum length: 28

config custom-message

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config device-detection-portal

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config fortiguard-wf

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config ftp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config http

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config icap

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config mail

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	

Parameter	Description	Type	Size
msg-type	Message type.	string	Maximum length: 28

config nac-quar

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config nntp

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config spam

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config sslvpn

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config traffic-quota

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config utm

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	
msg-type	Message type.	string	Maximum length: 28

config webproxy

Parameter	Description	Type	Size
buffer	Message string.	var-string	Maximum length: 32768
format	Format flag.	option	-
	Option	Description	
	<i>none</i>	No format type.	
	<i>text</i>	Text format.	
	<i>html</i>	HTML format.	
header	Header flag.	option	-
	Option	Description	
	<i>none</i>	No header type.	
	<i>http</i>	HTTP	
	<i>8bit</i>	8 bit.	

Parameter	Description	Type	Size
msg-type	Message type.	string	Maximum length: 28

config system replacemsg-image

Configure replacement message images.

```
config system replacemsg-image
    Description: Configure replacement message images.
    edit <name>
        set image-base64 {var-string}
        set image-type [gif|jpg|...]
    next
end
```

config system replacemsg-image

Parameter	Description	Type	Size
image-base64	Image data.	var-string	Maximum length: 32768
image-type	Image type.	option	-
	Option	Description	
	<i>gif</i>	GIF image.	
	<i>jpg</i>	JPEG image.	
	<i>tiff</i>	TIFF image.	
	<i>png</i>	PNG image.	
name	Image name.	string	Maximum length: 23

config system resource-limits

Configure resource limits.

```
config system resource-limits
    Description: Configure resource limits.
    set custom-service {integer}
    set dialup-tunnel {integer}
    set firewall-address {integer}
    set firewall-addrgrp {integer}
    set firewall-policy {integer}
```

```

set ipsec-phase1 {integer}
set ipsec-phase1-interface {integer}
set ipsec-phase2 {integer}
set ipsec-phase2-interface {integer}
set log-disk-quota {integer}
set onetime-schedule {integer}
set proxy {integer}
set recurring-schedule {integer}
set service-group {integer}
set session {integer}
set sslvpn {integer}
set user {integer}
set user-group {integer}
end

```

config system resource-limits

Parameter	Description	Type	Size
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295
dialup-tunnel	Maximum number of dial-up tunnels.	integer	Minimum value: 0 Maximum value: 4294967295
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295
firewall-addgrp	Maximum number of firewall address groups (IPv4, IPv6).	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

Parameter	Description	Type	Size
ipsec-phase1	Maximum number of VPN IPsec phase1 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295
ipsec-phase2	Maximum number of VPN IPsec phase2 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295
ipsec-phase2-interface	Maximum number of VPN IPsec phase2 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295
log-disk-quota	Log disk quota in megabytes (MB).	integer	Minimum value: 0 Maximum value: 4294967295 **
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295
recurring-schedule	Maximum number of firewall recurring schedules.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295
session	Maximum number of sessions.	integer	Minimum value: 0 Maximum value: 4294967295
sslvpn	Maximum number of SSL-VPN.	integer	Minimum value: 0 Maximum value: 4294967295
user	Maximum number of local users.	integer	Minimum value: 0 Maximum value: 4294967295
user-group	Maximum number of user groups.	integer	Minimum value: 0 Maximum value: 4294967295

** Values may differ between models.

config system saml

Global settings for SAML authentication.

```
config system saml
    Description: Global settings for SAML authentication.
    set cert {string}
    set default-login-page [normal|sso]
    set default-profile {string}
    set entity-id {string}
    set idp-cert {string}
    set idp-entity-id {string}
    set idp-single-logout-url {string}
    set idp-single-sign-on-url {string}
    set life {integer}
    set portal-url {string}
    set role [identity-provider|service-provider]
    set server-address {string}
```

```

config service-providers
  Description: Authorized service providers.
  edit <name>
    config assertion-attributes
      Description: Customized SAML attributes to send along with assertion.
      edit <name>
        set type [username|email]
      next
    end
    set idp-entity-id {string}
    set idp-single-logout-url {string}
    set idp-single-sign-on-url {string}
    set prefix {string}
    set sp-cert {string}
    set sp-entity-id {string}
    set sp-portal-url {string}
    set sp-single-logout-url {string}
    set sp-single-sign-on-url {string}
  next
end
set single-logout-url {string}
set single-sign-on-url {string}
set status [enable|disable]
set tolerance {integer}
end

```

config system saml

Parameter	Description	Type	Size
cert	Certificate to sign SAML messages.	string	Maximum length: 35
default-login-page	Choose default login page.	option	-
	Option	Description	
	<i>normal</i>	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
entity-id	SP entity ID. Read-only.	string	Maximum length: 255
idp-cert	IDP certificate name.	string	Maximum length: 35
idp-entity-id	IDP entity ID.	string	Maximum length: 255

Parameter	Description	Type	Size
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295
portal-url	SP portal URL. Read-only.	string	Maximum length: 255
role	SAML role.	option	-

Option	Description
<i>identity-provider</i>	Identity Provider.
<i>service-provider</i>	Service Provider.

server-address	Server address.	string	Maximum length: 63
single-logout-url	SP single logout URL. Read-only.	string	Maximum length: 255
single-sign-on-url	SP single sign-on URL. Read-only.	string	Maximum length: 255
status	Enable/disable SAML authentication (default = disable).	option	-

Option	Description
<i>enable</i>	Enable SAML authentication.
<i>disable</i>	Disable SAML authentication.

tolerance	Tolerance to 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
idp-entity-id	IDP entity ID. Read-only.	string	Maximum length: 255
idp-single-logout-url	IDP single logout URL. Read-only.	string	Maximum length: 255
idp-single-sign-on-url	IDP single sign-on URL. Read-only.	string	Maximum length: 255
name	Name.	string	Maximum length: 35
prefix	Prefix.	string	Maximum length: 35
sp-cert	SP certificate name.	string	Maximum length: 35
sp-entity-id	SP entity ID.	string	Maximum length: 255
sp-portal-url	SP portal URL.	string	Maximum length: 255
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255

config assertion-attributes

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 35
type	Type.	option	-
	Option	Description	
	username	User Name.	
	email	Email address.	

config system sdn-connector

Configure connection to SDN Connector.

```

config system sdn-connector
    Description: Configure connection to SDN Connector.
    edit <name>
        set access-key {string}
        set azure-region [global|china|...]
        set client-id {string}
        set client-secret {password}
        set compartment-id {string}
        set domain {string}
        config external-ip
            Description: Configure GCP external IP.
            edit <name>
                next
            end
        set gcp-project {string}
        set group-name {string}
        set ha-status [disable|enable]
        set login-endpoint {string}
        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
        set oci-cert {string}
        set oci-fingerprint {string}
        set oci-region {string}
        set oci-region-type [commercial|government]
        set password {password_aes256}
        set private-key {user}
        set region {string}
        set resource-group {string}
        set resource-url {string}
        config route
            Description: Configure GCP route.
            edit <name>
                next
            end
        config route-table
            Description: Configure Azure route table.
            edit <name>
                set resource-group {string}
                config route
                    Description: Configure Azure route.
                    edit <name>
                        set next-hop {string}
                    next
                end
                set subscription-id {string}
            next
        end
    next
end

```



```

end
set secret-key {password}
set secret-token {user}
set server {string}
set server-port {integer}
set service-account {string}
set status [disable|enable]
set subscription-id {string}
set tenant-id {string}
set type [aci|alicloud|...]
set update-interval {integer}
set use-metadata-iam [disable|enable]
set user-id {string}
set username {string}
set vpc-id {string}
next
end

```

config system sdn-connector

Parameter	Description	Type	Size
access-key	AWS / ACS access key ID.	string	Maximum length: 31
azure-region	Azure server region.	option	-
	Option	Description	
	<i>global</i>	Global Azure Server.	
	<i>china</i>	China Azure Server.	
	<i>germany</i>	Germany Azure Server.	
	<i>usgov</i>	US Government Azure Server.	
	<i>local</i>	Azure Stack Local Server.	
client-id	Azure client ID (application ID).	string	Maximum length: 63
client-secret	Azure client secret (application key).	password	Not Specified
compartment-id	Compartment ID.	string	Maximum length: 127
domain	Domain name.	string	Maximum length: 127
gcp-project	GCP project name.	string	Maximum length: 127
group-name	Group name of computers.	string	Maximum length: 127

Parameter	Description	Type	Size
ha-status	Enable/disable use for FortiGate HA service.	option	-
	Option	Description	
	<i>disable</i>	Disable use for FortiGate HA service.	
	<i>enable</i>	Enable use for FortiGate HA service.	
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127
name	SDN connector name.	string	Maximum length: 35
oci-cert	OCI certificate.	string	Maximum length: 63
oci-fingerprint	OCI pubkey fingerprint. Read-only.	string	Maximum length: 63
oci-region	OCI server region.	string	Maximum length: 31
oci-region-type	OCI region type.	option	-
	Option	Description	
	<i>commercial</i>	Commercial region.	
	<i>government</i>	Government region.	
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified
private-key	Private key of GCP service account.	user	Not Specified
region	AWS / ACS region name.	string	Maximum length: 31
resource-group	Azure resource group.	string	Maximum length: 63
resource-url	Azure Stack resource URL.	string	Maximum length: 127
secret-key	AWS / ACS secret access key.	password	Not Specified
secret-token	Secret token of Kubernetes service account.	user	Not Specified
server	Server address of the remote SDN connector.	string	Maximum length: 127

Parameter	Description	Type	Size
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535
service-account	GCP service account email.	string	Maximum length: 127
status	Enable/disable connection to the remote SDN connector.	option	-

Option	Description
<i>disable</i>	Disable connection to this SDN Connector.
<i>enable</i>	Enable connection to this SDN Connector.

subscription-id	Azure subscription ID.	string	Maximum length: 63
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127
type	Type of SDN connector.	option	-

Option	Description
<i>aci</i>	Application Centric Infrastructure (ACI).
<i>alicloud</i>	AliCloud Service (ACS).
<i>aws</i>	Amazon Web Services (AWS).
<i>azure</i>	Microsoft Azure.
<i>gcp</i>	Google Cloud Platform (GCP).
<i>nsx</i>	VMware NSX.
<i>nuage</i>	Nuage VSP.
<i>oci</i>	Oracle Cloud Infrastructure.
<i>openstack</i>	OpenStack.
<i>kubernetes</i>	Kubernetes.
<i>vmware</i>	VMware vSphere (vCenter & ESXi).
<i>sepm</i>	Symantec Endpoint Protection Manager.

update-interval	Dynamic object update interval (30 - 3600 sec, default = 60, 0 = disabled).	integer	Minimum value: 0 Maximum value: 3600

Parameter	Description	Type	Size
use-metadata-iam	Enable/disable using IAM role from metadata to call API.	option	-
	Option	Description	
	<i>disable</i>	Disable using IAM role to call API.	
	<i>enable</i>	Enable using IAM role to call API.	
user-id	User ID.	string	Maximum length: 127
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64
vpc-id	AWS VPC ID.	string	Maximum length: 31

config external-ip

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

config nic

Parameter	Description	Type	Size
name	Network interface name.	string	Maximum length: 63

config ip

Parameter	Description	Type	Size
name	IP configuration name.	string	Maximum length: 63
public-ip	Public IP name.	string	Maximum length: 63
resource-group	Resource group of Azure public IP.	string	Maximum length: 63

config route

Parameter	Description	Type	Size
name	Route name.	string	Maximum length: 63

config route-table

Parameter	Description	Type	Size
name	Route table name.	string	Maximum length: 63
resource-group	Resource group of Azure route table.	string	Maximum length: 63
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63

config route

Parameter	Description	Type	Size
name	Route name.	string	Maximum length: 63
next-hop	Next hop address.	string	Maximum length: 127

config system session-helper

Configure session helper.

```
config system session-helper
  Description: Configure session helper.
  edit <id>
    set name [ftp|tftp|...]
    set port {integer}
    set protocol {integer}
  next
end
```

config system session-helper

Parameter	Description	Type	Size																																
id	Session helper ID.	integer	Minimum value: 0 Maximum value: 4294967295																																
name	Helper name.	option	-																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>tftp</i></td><td>TFTP.</td></tr><tr><td><i>ras</i></td><td>RAS.</td></tr><tr><td><i>h323</i></td><td>H323.</td></tr><tr><td><i>tns</i></td><td>TNS.</td></tr><tr><td><i>mms</i></td><td>MMS.</td></tr><tr><td><i>sip</i></td><td>SIP.</td></tr><tr><td><i>pptp</i></td><td>PPTP.</td></tr><tr><td><i>rtsp</i></td><td>RTSP.</td></tr><tr><td><i>dns-udp</i></td><td>DNS UDP.</td></tr><tr><td><i>dns-tcp</i></td><td>DNS TCP.</td></tr><tr><td><i>pmap</i></td><td>PMAP.</td></tr><tr><td><i>rsh</i></td><td>RSH.</td></tr><tr><td><i>dcerpc</i></td><td>DCERPC.</td></tr><tr><td><i>mgcp</i></td><td>MGCP.</td></tr></table>	Option	Description	<i>ftp</i>	FTP.	<i>tftp</i>	TFTP.	<i>ras</i>	RAS.	<i>h323</i>	H323.	<i>tns</i>	TNS.	<i>mms</i>	MMS.	<i>sip</i>	SIP.	<i>pptp</i>	PPTP.	<i>rtsp</i>	RTSP.	<i>dns-udp</i>	DNS UDP.	<i>dns-tcp</i>	DNS TCP.	<i>pmap</i>	PMAP.	<i>rsh</i>	RSH.	<i>dcerpc</i>	DCERPC.	<i>mgcp</i>	MGCP.		
	Option	Description																																	
	<i>ftp</i>	FTP.																																	
	<i>tftp</i>	TFTP.																																	
	<i>ras</i>	RAS.																																	
	<i>h323</i>	H323.																																	
	<i>tns</i>	TNS.																																	
	<i>mms</i>	MMS.																																	
	<i>sip</i>	SIP.																																	
	<i>pptp</i>	PPTP.																																	
	<i>rtsp</i>	RTSP.																																	
	<i>dns-udp</i>	DNS UDP.																																	
	<i>dns-tcp</i>	DNS TCP.																																	
	<i>pmap</i>	PMAP.																																	
	<i>rsh</i>	RSH.																																	
<i>dcerpc</i>	DCERPC.																																		
<i>mgcp</i>	MGCP.																																		
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535																																
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255																																

config system session-ttl

Configure global session TTL timers for this FortiGate.

```
config system session-ttl
  Description: Configure global session TTL timers for this FortiGate.
  set default {user}
  config port
    Description: Session TTL port.
    edit <id>
      set end-port {integer}
      set protocol {integer}
      set start-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
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535
id	Table entry ID.	integer	Minimum value: 0 Maximum value: 65535
protocol	Protocol (0 - 255).	integer	Minimum value: 0 Maximum value: 255
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535
timeout	Session timeout (TTL).	user	Not Specified

config system settings

Configure VDOM settings.

```
config system settings
  Description: Configure VDOM settings.
  set allow-linkdown-path [enable|disable]
  set allow-subnet-overlap [enable|disable]
  set asymroute [enable|disable]
  set asymroute-icmp [enable|disable]
  set asymroute6 [enable|disable]
  set asymroute6-icmp [enable|disable]
  set auxiliary-session [enable|disable]
  set bfd [enable|disable]
  set bfd-desired-min-tx {integer}
  set bfd-detect-mult {integer}
  set bfd-dont-enforce-src-port [enable|disable]
  set bfd-required-min-rx {integer}
  set block-land-attack [disable|enable]
  set central-nat [enable|disable]
  set comments {var-string}
  set consolidated-firewall-mode [enable|disable]
  set default-voip-alg-mode [proxy-based|kernel-helper-based]
  set deny-tcp-with-icmp [enable|disable]
  set device {string}
  set dhcp-proxy [enable|disable]
  set dhcp-proxy-interface {string}
  set dhcp-proxy-interface-select-method [auto|sdwan|...]
  set dhcp-server-ip {user}
  set dhcp6-server-ip {user}
  set discovered-device-timeout {integer}
  set ecmp-max-paths {integer}
  set email-portal-check-dns [disable|enable]
  set firewall-session-dirty [check-all|check-new|...]
  set fw-session-hairpin [enable|disable]
  set gateway {ipv4-address}
  set gateway6 {ipv6-address}
  set gui-advanced-policy [enable|disable]
  set gui-allow-unnamed-policy [enable|disable]
  set gui-antivirus [enable|disable]
  set gui-ap-profile [enable|disable]
  set gui-application-control [enable|disable]
  set gui-default-policy-columns <name1>, <name2>, ...
  set gui-dhcp-advanced [enable|disable]
  set gui-dns-database [enable|disable]
  set gui-dnsfilter [enable|disable]
  set gui-domain-ip-reputation [enable|disable]
  set gui-dos-policy [enable|disable]
  set gui-dynamic-profile-display [enable|disable]
  set gui-dynamic-routing [enable|disable]
  set gui-email-collection [enable|disable]
  set gui-endpoint-control [enable|disable]
  set gui-endpoint-control-advanced [enable|disable]
  set gui-explicit-proxy [enable|disable]
  set gui-fortiap-split-tunneling [enable|disable]
```

```
set gui-fortiextender-controller [enable|disable]
set gui-icap [enable|disable]
set gui-implicit-policy [enable|disable]
set gui-ips [enable|disable]
set gui-load-balance [enable|disable]
set gui-local-in-policy [enable|disable]
set gui-local-reports [enable|disable]
set gui-multicast-policy [enable|disable]
set gui-multiple-interface-policy [enable|disable]
set gui-multiple-utm-profiles [enable|disable]
set gui-nat46-64 [enable|disable]
set gui-object-colors [enable|disable]
set gui-per-policy-disclaimer [enable|disable]
set gui-policy-based-ipsec [enable|disable]
set gui-replacement-message-groups [enable|disable]
set gui-spamfilter [enable|disable]
set gui-sslvpn-personal-bookmarks [enable|disable]
set gui-sslvpn-realms [enable|disable]
set gui-switch-controller [enable|disable]
set gui-threat-weight [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-voip-profile [enable|disable]
set gui-vpn [enable|disable]
set gui-waf-profile [enable|disable]
set gui-wan-load-balancing [enable|disable]
set gui-wanopt-cache [enable|disable]
set gui-webfilter [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-wireless-controller [enable|disable]
set http-external-dest [fortiweb|forticache]
set ike-dn-format [with-space|no-space]
set ike-quick-crash-detect [enable|disable]
set ike-session-resume [enable|disable]
set implicit-allow-dns [enable|disable]
set ip {ipv4-classnet-host}
set ip6 {ipv6-prefix}
set link-down-access [enable|disable]
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set mac-ttl {integer}
set manageip {user}
set manageip6 {ipv6-prefix}
set multicast-forward [enable|disable]
set multicast-skip-policy [enable|disable]
set multicast-ttl-notchange [enable|disable]
set ngfw-mode [profile-based|policy-based]
set opmode [nat|transparent]
set prp-trailer-action [enable|disable]
set sccp-port {integer}
set sctp-session-without-init [enable|disable]
set ses-denied-traffic [enable|disable]
set sip-expectation [enable|disable]
set sip-nat-trace [enable|disable]
set sip-ssl-port {integer}
set sip-tcp-port {integer}
set sip-udp-port {integer}
```

```

set snat-hairpin-traffic [enable|disable]
set status [enable|disable]
set strict-src-check [enable|disable]
set tcp-session-without-syn [enable|disable]
set utf8-spam-tagging [enable|disable]
set v4-ecmp-mode [source-ip-based|weight-based|...]
set vpn-stats-log {option1}, {option2}, ...
set vpn-stats-period {integer}
set wccp-cache-engine [enable|disable]

```

end

config system settings

Parameter	Description	Type	Size
allow-linkdown-path	Enable/disable link down path.	option	-
	Option	Description	
	<i>enable</i>	Allow link down path.	
	<i>disable</i>	Do not allow link down path.	
allow-subnet-overlap	Enable/disable allowing interface subnets to use overlapping IP addresses.	option	-
	Option	Description	
	<i>enable</i>	Enable overlapping subnets.	
	<i>disable</i>	Disable overlapping subnets.	
asymroute	Enable/disable IPv4 asymmetric routing.	option	-
	Option	Description	
	<i>enable</i>	Enable IPv4 asymmetric routing.	
	<i>disable</i>	Disable IPv4 asymmetric routing.	
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-
	Option	Description	
	<i>enable</i>	Enable ICMP asymmetric routing.	
	<i>disable</i>	Disable ICMP asymmetric routing.	
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable asymmetric IPv6 routing.</td></tr><tr><td><i>disable</i></td><td>Disable asymmetric IPv6 routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable asymmetric IPv6 routing.	<i>disable</i>	Disable asymmetric IPv6 routing.		
Option	Description								
<i>enable</i>	Enable asymmetric IPv6 routing.								
<i>disable</i>	Disable asymmetric IPv6 routing.								
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable asymmetric ICMPv6 routing.</td></tr><tr><td><i>disable</i></td><td>Disable asymmetric ICMPv6 routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable asymmetric ICMPv6 routing.	<i>disable</i>	Disable asymmetric ICMPv6 routing.		
Option	Description								
<i>enable</i>	Enable asymmetric ICMPv6 routing.								
<i>disable</i>	Disable asymmetric ICMPv6 routing.								
auxiliary-session *	Enable/disable auxiliary session.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auxiliary session for this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable auxiliary session for this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable auxiliary session for this VDOM.	<i>disable</i>	Disable auxiliary session for this VDOM.		
Option	Description								
<i>enable</i>	Enable auxiliary session for this VDOM.								
<i>disable</i>	Disable auxiliary session for this VDOM.								
bfd	Enable/disable Bi-directional Forwarding Detection (BFD) on all interfaces.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Bi-directional Forwarding Detection (BFD) on all interfaces.</td></tr><tr><td><i>disable</i></td><td>Disable Bi-directional Forwarding Detection (BFD) on all interfaces.</td></tr></table>	Option	Description	<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.	<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.		
Option	Description								
<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.								
<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.								
bfd-desired-min-tx	BFD desired minimal transmit interval (1 - 100000 ms, default = 50).	integer	Minimum value: 1 Maximum value: 100000						
bfd-detect-mult	BFD detection multiplier (1 - 50, default = 3).	integer	Minimum value: 1 Maximum value: 50						
bfd-dont-enforce-src-port	Enable to not enforce verifying the source port of BFD Packets.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verifying the source port of BFD Packets.</td></tr><tr><td><i>disable</i></td><td>Disable verifying the source port of BFD Packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable verifying the source port of BFD Packets.	<i>disable</i>	Disable verifying the source port of BFD Packets.		
Option	Description								
<i>enable</i>	Enable verifying the source port of BFD Packets.								
<i>disable</i>	Disable verifying the source port of BFD Packets.								

Parameter	Description	Type	Size						
bfd-required-min-rx	BFD required minimal receive interval (1 - 100000 ms, default = 50).	integer	Minimum value: 1 Maximum value: 100000						
block-land-attack	Enable/disable blocking of land attacks.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not block land attack.</td></tr><tr><td><i>enable</i></td><td>Block land attack.</td></tr></table>	Option	Description	<i>disable</i>	Do not block land attack.	<i>enable</i>	Block land attack.		
Option	Description								
<i>disable</i>	Do not block land attack.								
<i>enable</i>	Block land attack.								
central-nat	Enable/disable central NAT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable central NAT.</td></tr><tr><td><i>disable</i></td><td>Disable central NAT.</td></tr></table>	Option	Description	<i>enable</i>	Enable central NAT.	<i>disable</i>	Disable central NAT.		
Option	Description								
<i>enable</i>	Enable central NAT.								
<i>disable</i>	Disable central NAT.								
comments	VDOM comments.	var-string	Maximum length: 255						
consolidated-firewall-mode	Consolidated firewall mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable consolidated firewall mode.</td></tr><tr><td><i>disable</i></td><td>Disable consolidated firewall mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable consolidated firewall mode.	<i>disable</i>	Disable consolidated firewall mode.		
Option	Description								
<i>enable</i>	Enable consolidated firewall mode.								
<i>disable</i>	Disable consolidated firewall mode.								
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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>proxy-based</i></td><td>Use a default proxy-based VoIP ALG.</td></tr><tr><td><i>kernel-helper-based</i></td><td>Use the SIP session helper.</td></tr></table>	Option	Description	<i>proxy-based</i>	Use a default proxy-based VoIP ALG.	<i>kernel-helper-based</i>	Use the SIP session helper.		
Option	Description								
<i>proxy-based</i>	Use a default proxy-based VoIP ALG.								
<i>kernel-helper-based</i>	Use the SIP session helper.								
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Deny TCP with ICMP.</td></tr><tr><td><i>disable</i></td><td>Disable denying TCP with ICMP.</td></tr></table>	Option	Description	<i>enable</i>	Deny TCP with ICMP.	<i>disable</i>	Disable denying TCP with ICMP.		
Option	Description								
<i>enable</i>	Deny TCP with ICMP.								
<i>disable</i>	Disable denying TCP with ICMP.								

Parameter	Description	Type	Size
device	Interface to use for management access for NAT mode.	string	Maximum length: 35
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-
	Option	Description	
	<i>enable</i>	Enable the DHCP proxy.	
	<i>disable</i>	Disable the DHCP proxy.	
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified
discovered-device-timeout	Timeout for discovered devices (1 - 365 days, default = 28).	integer	Minimum value: 1 Maximum value: 365
ecmp-max-paths	Maximum number of Equal Cost Multi-Path (ECMP) next-hops. Set to 1 to disable ECMP routing (1 - 255, default = 255).	integer	Minimum value: 1 Maximum value: 255
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-
	Option	Description	
	<i>disable</i>	Disable email address checking with DNS.	
	<i>enable</i>	Enable email address checking with DNS.	
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>check-all</i>	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.	
	<i>check-new</i>	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.	
	<i>check-policy-option</i>	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.	
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiGate.	option	-
	Option	Description	
	<i>enable</i>	Perform a policy check every time.	
	<i>disable</i>	Perform a policy check only the first time the session is received.	
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified
gateway6	Transparent mode IPv6 default gateway IP address.	ipv6-address	Not Specified
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable advanced policy configuration on the GUI.	
	<i>disable</i>	Disable advanced policy configuration on the GUI.	
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable the requirement for policy naming on the GUI.	
	<i>disable</i>	Disable the requirement for policy naming on the GUI.	
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable AntiVirus on the GUI.	
	<i>disable</i>	Disable AntiVirus on the GUI.	
gui-ap-profile	Enable/disable FortiAP profiles on the GUI.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAP profiles on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAP profiles on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAP profiles on the GUI.	<i>disable</i>	Disable FortiAP profiles on the GUI.		
Option	Description								
<i>enable</i>	Enable FortiAP profiles on the GUI.								
<i>disable</i>	Disable FortiAP profiles on the GUI.								
gui-application-control	Enable/disable application control on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application control on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable application control on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable application control on the GUI.	<i>disable</i>	Disable application control on the GUI.		
Option	Description								
<i>enable</i>	Enable application control on the GUI.								
<i>disable</i>	Disable application control on the GUI.								
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79						
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable advanced DHCP options on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable advanced DHCP options on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable advanced DHCP options on the GUI.	<i>disable</i>	Disable advanced DHCP options on the GUI.		
Option	Description								
<i>enable</i>	Enable advanced DHCP options on the GUI.								
<i>disable</i>	Disable advanced DHCP options on the GUI.								
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS database settings on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable DNS database settings on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNS database settings on the GUI.	<i>disable</i>	Disable DNS database settings on the GUI.		
Option	Description								
<i>enable</i>	Enable DNS database settings on the GUI.								
<i>disable</i>	Disable DNS database settings on the GUI.								
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS Filtering on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable DNS Filtering on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNS Filtering on the GUI.	<i>disable</i>	Disable DNS Filtering on the GUI.		
Option	Description								
<i>enable</i>	Enable DNS Filtering on the GUI.								
<i>disable</i>	Disable DNS Filtering on the GUI.								
gui-domain-ip-reputation	Enable/disable Domain and IP Reputation on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Domain and IP Reputation on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Domain and IP Reputation on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Domain and IP Reputation on the GUI.	<i>disable</i>	Disable Domain and IP Reputation on the GUI.		
Option	Description								
<i>enable</i>	Enable Domain and IP Reputation on the GUI.								
<i>disable</i>	Disable Domain and IP Reputation on the GUI.								

Parameter	Description	Type	Size						
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DoS policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable DoS policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DoS policies on the GUI.	<i>disable</i>	Disable DoS policies on the GUI.		
Option	Description								
<i>enable</i>	Enable DoS policies on the GUI.								
<i>disable</i>	Disable DoS policies on the GUI.								
gui-dynamic-profile-display	Enable/disable RADIUS Single Sign On (RSSO) on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS Single Sign On (RSSO) on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS Single Sign On (RSSO) on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS Single Sign On (RSSO) on the GUI.	<i>disable</i>	Disable RADIUS Single Sign On (RSSO) on the GUI.		
Option	Description								
<i>enable</i>	Enable RADIUS Single Sign On (RSSO) on the GUI.								
<i>disable</i>	Disable RADIUS Single Sign On (RSSO) on the GUI.								
gui-dynamic-routing	Enable/disable dynamic routing on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic routing on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic routing on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic routing on the GUI.	<i>disable</i>	Disable dynamic routing on the GUI.		
Option	Description								
<i>enable</i>	Enable dynamic routing on the GUI.								
<i>disable</i>	Disable dynamic routing on the GUI.								
gui-email-collection	Enable/disable email collection on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable email collection on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable email collection on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable email collection on the GUI.	<i>disable</i>	Disable email collection on the GUI.		
Option	Description								
<i>enable</i>	Enable email collection on the GUI.								
<i>disable</i>	Disable email collection on the GUI.								
gui-endpoint-control	Enable/disable endpoint control on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable endpoint control on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable endpoint control on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable endpoint control on the GUI.	<i>disable</i>	Disable endpoint control on the GUI.		
Option	Description								
<i>enable</i>	Enable endpoint control on the GUI.								
<i>disable</i>	Disable endpoint control on the GUI.								
gui-endpoint-control-advanced	Enable/disable advanced endpoint control options on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable advanced endpoint control options on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable advanced endpoint control options on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable advanced endpoint control options on the GUI.	<i>disable</i>	Disable advanced endpoint control options on the GUI.		
Option	Description								
<i>enable</i>	Enable advanced endpoint control options on the GUI.								
<i>disable</i>	Disable advanced endpoint control options on the GUI.								

Parameter	Description	Type	Size						
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the explicit proxy on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit proxy on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable the explicit proxy on the GUI.	<i>disable</i>	Disable the explicit proxy on the GUI.		
Option	Description								
<i>enable</i>	Enable the explicit proxy on the GUI.								
<i>disable</i>	Disable the explicit proxy on the GUI.								
gui-fortiap-split-tunneling	Enable/disable FortiAP split tunneling on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAP split tunneling on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAP split tunneling on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAP split tunneling on the GUI.	<i>disable</i>	Disable FortiAP split tunneling on the GUI.		
Option	Description								
<i>enable</i>	Enable FortiAP split tunneling on the GUI.								
<i>disable</i>	Disable FortiAP split tunneling on the GUI.								
gui-fortiextender-controller	Enable/disable FortiExtender on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiExtender on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable FortiExtender on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiExtender on the GUI.	<i>disable</i>	Disable FortiExtender on the GUI.		
Option	Description								
<i>enable</i>	Enable FortiExtender on the GUI.								
<i>disable</i>	Disable FortiExtender on the GUI.								
gui-icap	Enable/disable ICAP on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICAP on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable ICAP on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICAP on the GUI.	<i>disable</i>	Disable ICAP on the GUI.		
Option	Description								
<i>enable</i>	Enable ICAP on the GUI.								
<i>disable</i>	Disable ICAP on the GUI.								
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable implicit firewall policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable implicit firewall policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable implicit firewall policies on the GUI.	<i>disable</i>	Disable implicit firewall policies on the GUI.		
Option	Description								
<i>enable</i>	Enable implicit firewall policies on the GUI.								
<i>disable</i>	Disable implicit firewall policies on the GUI.								
gui-ips	Enable/disable IPS on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable IPS on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS on the GUI.	<i>disable</i>	Disable IPS on the GUI.		
Option	Description								
<i>enable</i>	Enable IPS on the GUI.								
<i>disable</i>	Disable IPS on the GUI.								

Parameter	Description	Type	Size

gui-load-balance	Enable/disable server load balancing on the GUI.	option	-

Option	Description
<i>enable</i>	Enable server load balancing on the GUI.
<i>disable</i>	Disable server load balancing on the GUI.

gui-local-in-policy	Enable/disable Local-In policies on the GUI.	option	-

Option	Description
<i>enable</i>	Enable Local-In policies on the GUI.
<i>disable</i>	Disable Local-In policies on the GUI.

gui-local-reports *	Enable/disable local reports on the GUI.	option	-

Option	Description
<i>enable</i>	Enable local reports on the GUI.
<i>disable</i>	Disable local reports on the GUI.

gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-

Option	Description
<i>enable</i>	Enable multicast firewall policies on the GUI.
<i>disable</i>	Disable multicast firewall policies on the GUI.

gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-

Option	Description
<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.
<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.

gui-multiple-utm-profiles	Enable/disable multiple UTM profiles on the GUI.	option	-

Option	Description
<i>enable</i>	Enable multiple UTM profiles on the GUI.
<i>disable</i>	Disable multiple UTM profiles on the GUI.

Parameter	Description	Type	Size						
gui-nat46-64	Enable/disable NAT46 and NAT64 settings on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAT46 and NAT64 settings on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable NAT46 and NAT64 settings on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable NAT46 and NAT64 settings on the GUI.	<i>disable</i>	Disable NAT46 and NAT64 settings on the GUI.		
Option	Description								
<i>enable</i>	Enable NAT46 and NAT64 settings on the GUI.								
<i>disable</i>	Disable NAT46 and NAT64 settings on the GUI.								
gui-object-colors	Enable/disable object colors on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable object colors on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable object colors on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable object colors on the GUI.	<i>disable</i>	Disable object colors on the GUI.		
Option	Description								
<i>enable</i>	Enable object colors on the GUI.								
<i>disable</i>	Disable object colors on the GUI.								
gui-per-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy disclaimer on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable policy disclaimer on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy disclaimer on the GUI.	<i>disable</i>	Disable policy disclaimer on the GUI.		
Option	Description								
<i>enable</i>	Enable policy disclaimer on the GUI.								
<i>disable</i>	Disable policy disclaimer on the GUI.								
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy-based IPsec VPN on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable policy-based IPsec VPN on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy-based IPsec VPN on the GUI.	<i>disable</i>	Disable policy-based IPsec VPN on the GUI.		
Option	Description								
<i>enable</i>	Enable policy-based IPsec VPN on the GUI.								
<i>disable</i>	Disable policy-based IPsec VPN on the GUI.								
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable replacement message groups on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable replacement message groups on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable replacement message groups on the GUI.	<i>disable</i>	Disable replacement message groups on the GUI.		
Option	Description								
<i>enable</i>	Enable replacement message groups on the GUI.								
<i>disable</i>	Disable replacement message groups on the GUI.								
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Antispam on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Antispam on the GUI.				
Option	Description								
<i>enable</i>	Enable Antispam on the GUI.								

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable Antispam on the GUI.	
gui-sslvpn-personal-bookmarks	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL-VPN personal bookmark management on the GUI.	
	<i>disable</i>	Disable SSL-VPN personal bookmark management on the GUI.	
gui-sslvpn-realms	Enable/disable SSL-VPN realms on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable SSL-VPN realms on the GUI.	
	<i>disable</i>	Disable SSL-VPN realms on the GUI.	
gui-switch-controller *	Enable/disable the switch controller on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable the switch controller on the GUI.	
	<i>disable</i>	Disable the switch controller on the GUI.	
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable threat weight on the GUI.	
	<i>disable</i>	Disable threat weight on the GUI.	
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable traffic shaping on the GUI.	
	<i>disable</i>	Disable traffic shaping on the GUI.	
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable VoIP profiles on the GUI.	
	<i>disable</i>	Disable VoIP profiles on the GUI.	
gui-vpn	Enable/disable VPN tunnels on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable VPN tunnels on the GUI.	
	<i>disable</i>	Disable VPN tunnels on the GUI.	
gui-waf-profile	Enable/disable Web Application Firewall on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable Web Application Firewall on the GUI.	
	<i>disable</i>	Disable Web Application Firewall on the GUI.	
gui-wan-load-balancing	Enable/disable SD-WAN on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable SD-WAN on the GUI.	
	<i>disable</i>	Disable SD-WAN on the GUI.	
gui-wanopt-cache *	Enable/disable WAN Optimization and Web Caching on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable WAN Optimization and Web Caching on the GUI.	
	<i>disable</i>	Disable WAN Optimization and Web Caching on the GUI.	
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable Web filtering on the GUI.	
	<i>disable</i>	Disable Web filtering on the GUI.	
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable advanced web filtering on the GUI.	
	<i>disable</i>	Disable advanced web filtering on the GUI.	
gui-wireless-controller	Enable/disable the wireless controller on the GUI.	option	-
	Option	Description	
	<i>enable</i>	Enable the wireless controller on the GUI.	
	<i>disable</i>	Disable the wireless controller on the GUI.	
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-
	Option	Description	
	<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.	
	<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.	
ike-dn-format	Configure IKE ASN.1 Distinguished Name format conventions.	option	-
	Option	Description	
	<i>with-space</i>	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.	
	<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.	
ike-quick-crash-detect	Enable/disable IKE quick crash detection (RFC 6290).	option	-
	Option	Description	
	<i>enable</i>	Enable IKE quick crash detection (RFC 6290).	
	<i>disable</i>	Disable IKE quick crash detection (RFC 6290).	
ike-session-resume	Enable/disable IKEv2 session resumption (RFC 5723).	option	-
	Option	Description	
	<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).	
	<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).	

Parameter	Description	Type	Size								
implicit-allow-dns	Enable/disable implicitly allowing DNS traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable implicitly allowing DNS traffic.</td></tr><tr><td><i>disable</i></td><td>Disable implicitly allowing DNS traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable implicitly allowing DNS traffic.	<i>disable</i>	Disable implicitly allowing DNS traffic.				
Option	Description										
<i>enable</i>	Enable implicitly allowing DNS traffic.										
<i>disable</i>	Disable implicitly allowing DNS traffic.										
ip	IP address and netmask.	ipv4-classnet-host	Not Specified								
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified								
link-down-access	Enable/disable link down access traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow link down access traffic.</td></tr><tr><td><i>disable</i></td><td>Block link down access traffic.</td></tr></table>	Option	Description	<i>enable</i>	Allow link down access traffic.	<i>disable</i>	Block link down access traffic.				
Option	Description										
<i>enable</i>	Allow link down access traffic.										
<i>disable</i>	Block link down access traffic.										
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception for this VDOM or apply global settings to this VDOM.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable LLDP reception for this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable LLDP reception for this VDOM.</td></tr><tr><td><i>global</i></td><td>Use the global LLDP reception configuration for this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable LLDP reception for this VDOM.	<i>disable</i>	Disable LLDP reception for this VDOM.	<i>global</i>	Use the global LLDP reception configuration for this VDOM.		
Option	Description										
<i>enable</i>	Enable LLDP reception for this VDOM.										
<i>disable</i>	Disable LLDP reception for this VDOM.										
<i>global</i>	Use the global LLDP reception configuration for this VDOM.										
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission for this VDOM or apply global settings to this VDOM.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable LLDP transmission for this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable LLDP transmission for this VDOM.</td></tr><tr><td><i>global</i></td><td>Use the global LLDP transmission configuration for this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable LLDP transmission for this VDOM.	<i>disable</i>	Disable LLDP transmission for this VDOM.	<i>global</i>	Use the global LLDP transmission configuration for this VDOM.		
Option	Description										
<i>enable</i>	Enable LLDP transmission for this VDOM.										
<i>disable</i>	Disable LLDP transmission for this VDOM.										
<i>global</i>	Use the global LLDP transmission configuration for this VDOM.										
mac-ttl	Duration of MAC addresses in Transparent mode (300 - 8640000 sec, default = 300).	integer	Minimum value: 300 Maximum value: 8640000								

Parameter	Description	Type	Size
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified
multicast-forward	Enable/disable multicast forwarding.	option	-

Option	Description
<i>enable</i>	Enable multicast forwarding.
<i>disable</i>	Disable multicast forwarding.

multicast-skip-policy	Enable/disable allowing multicast traffic through the FortiGate without a policy check.	option	-

Option	Description
<i>enable</i>	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.
<i>disable</i>	Require a multicast policy to allow multicast traffic to pass through the FortiGate.

multicast-ttl-notchange	Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.	option	-

Option	Description
<i>enable</i>	The multicast TTL is not changed.
<i>disable</i>	The multicast TTL may be changed.

ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-

Option	Description
<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.
<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.

opmode	Firewall operation mode (NAT or Transparent).	option	-

Option	Description
<i>nat</i>	Change to NAT mode.
<i>transparent</i>	Change to transparent mode.

Parameter	Description	Type	Size						
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Try to keep PRP trailer.</td></tr><tr><td>disable</td><td>Trim PRP trailer.</td></tr></table>	Option	Description	enable	Try to keep PRP trailer.	disable	Trim PRP trailer.		
Option	Description								
enable	Try to keep PRP trailer.								
disable	Trim PRP trailer.								
sccp-port	TCP port the SCCP proxy monitors for SCCP traffic (0 - 65535, default = 2000).	integer	Minimum value: 0 Maximum value: 65535						
sctp-session-without-init	Enable/disable SCTP session creation without SCTP INIT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SCTP session creation without SCTP INIT.</td></tr><tr><td>disable</td><td>Disable SCTP session creation without SCTP INIT.</td></tr></table>	Option	Description	enable	Enable SCTP session creation without SCTP INIT.	disable	Disable SCTP session creation without SCTP INIT.		
Option	Description								
enable	Enable SCTP session creation without SCTP INIT.								
disable	Disable SCTP session creation without SCTP INIT.								
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Include denied sessions in the session table.</td></tr><tr><td>disable</td><td>Do not add denied sessions to the session table.</td></tr></table>	Option	Description	enable	Include denied sessions in the session table.	disable	Do not add denied sessions to the session table.		
Option	Description								
enable	Include denied sessions in the session table.								
disable	Do not add denied sessions to the session table.								
sip-expectation	Enable/disable the SIP kernel session helper to create an expectation for port 5060.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow SIP session helper to create an expectation for port 5060.</td></tr><tr><td>disable</td><td>Prevent SIP session helper from creating an expectation for port 5060.</td></tr></table>	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.		
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.								
sip-nat-trace	Enable/disable recording the original SIP source IP address when NAT is used.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Record the original SIP source IP address when NAT is used.</td></tr><tr><td>disable</td><td>Do not record the original SIP source IP address when NAT is used.</td></tr></table>	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.		
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						
sip-ssl-port *	TCP port the SIP proxy monitors for SIP SSL/TLS traffic (0 - 65535, default = 5061).	integer	Minimum value: 0 Maximum value: 65535						
sip-tcp-port	TCP port the SIP proxy monitors for SIP traffic (0 - 65535, default = 5060).	integer	Minimum value: 1 Maximum value: 65535						
sip-udp-port	UDP port the SIP proxy monitors for SIP traffic (0 - 65535, default = 5060).	integer	Minimum value: 1 Maximum value: 65535						
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SNAT for hairpin traffic.</td></tr><tr><td><i>disable</i></td><td>Disable SNAT for hairpin traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable SNAT for hairpin traffic.	<i>disable</i>	Disable SNAT for hairpin traffic.		
Option	Description								
<i>enable</i>	Enable SNAT for hairpin traffic.								
<i>disable</i>	Disable SNAT for hairpin traffic.								
status	Enable/disable this VDOM.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable this VDOM.	<i>disable</i>	Disable this VDOM.		
Option	Description								
<i>enable</i>	Enable this VDOM.								
<i>disable</i>	Disable this VDOM.								
strict-src-check	Enable/disable strict source verification.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict source verification.</td></tr><tr><td><i>disable</i></td><td>Disable strict source verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict source verification.	<i>disable</i>	Disable strict source verification.		
Option	Description								
<i>enable</i>	Enable strict source verification.								
<i>disable</i>	Disable strict source verification.								
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow TCP session without SYN flags.</td></tr><tr><td><i>disable</i></td><td>Do not allow TCP session without SYN flags.</td></tr></table>	Option	Description	<i>enable</i>	Allow TCP session without SYN flags.	<i>disable</i>	Do not allow TCP session without SYN flags.		
Option	Description								
<i>enable</i>	Allow TCP session without SYN flags.								
<i>disable</i>	Do not allow TCP session without SYN flags.								
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-						

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Convert antispam tags to UTF-8.</td></tr><tr><td><i>disable</i></td><td>Do not convert antispam tags.</td></tr></table>	Option	Description	<i>enable</i>	Convert antispam tags to UTF-8.	<i>disable</i>	Do not convert antispam tags.						
Option	Description												
<i>enable</i>	Convert antispam tags to UTF-8.												
<i>disable</i>	Do not convert antispam tags.												
v4-ecmp-mode	IPv4 Equal-cost multi-path (ECMP) routing and load balancing mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source-ip-based</i></td><td>Select next hop based on source IP.</td></tr><tr><td><i>weight-based</i></td><td>Select next hop based on weight.</td></tr><tr><td><i>usage-based</i></td><td>Select next hop based on usage.</td></tr><tr><td><i>source-dest-ip-based</i></td><td>Select next hop based on both source and destination IPs.</td></tr></table>	Option	Description	<i>source-ip-based</i>	Select next hop based on source IP.	<i>weight-based</i>	Select next hop based on weight.	<i>usage-based</i>	Select next hop based on usage.	<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.		
Option	Description												
<i>source-ip-based</i>	Select next hop based on source IP.												
<i>weight-based</i>	Select next hop based on weight.												
<i>usage-based</i>	Select next hop based on usage.												
<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.												
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipsec</i></td><td>IPsec.</td></tr><tr><td><i>pptp</i></td><td>PPTP.</td></tr><tr><td><i>l2tp</i></td><td>L2TP.</td></tr><tr><td><i>ssl</i></td><td>SSL.</td></tr></table>	Option	Description	<i>ipsec</i>	IPsec.	<i>pptp</i>	PPTP.	<i>l2tp</i>	L2TP.	<i>ssl</i>	SSL.		
Option	Description												
<i>ipsec</i>	IPsec.												
<i>pptp</i>	PPTP.												
<i>l2tp</i>	L2TP.												
<i>ssl</i>	SSL.												
vpn-stats-period	Period to send VPN log statistics (0 or 60 - 86400 sec).	integer	Minimum value: 0 Maximum value: 4294967295										
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP cache engine.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP cache engine.</td></tr></table>	Option	Description	<i>enable</i>	Enable WCCP cache engine.	<i>disable</i>	Disable WCCP cache engine.						
Option	Description												
<i>enable</i>	Enable WCCP cache engine.												
<i>disable</i>	Disable WCCP cache engine.												

* This parameter may not exist in some models.

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 (default = 0.0.0.0).	ipv4-address	Not Specified
collector-port	UDP port number used for sending sFlow datagrams (configure only if required by your sFlow collector or your network configuration) (0 - 65535, default = 6343).	integer	Minimum value: 0 Maximum value: 65535
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified

config system sit-tunnel

Configure IPv6 tunnel over IPv4.

```

config system sit-tunnel
    Description: Configure IPv6 tunnel over IPv4.
    edit <name>
        set auto-asic-offload [enable|disable]
        set destination {ipv4-address}
        set interface {string}
        set ip6 {ipv6-prefix}
        set source {ipv4-address}
    next
end

```

config system sit-tunnel

Parameter	Description	Type	Size						
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto ASIC offloading.</td></tr><tr><td><i>disable</i></td><td>Disable ASIC offloading.</td></tr></table>			Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.
Option	Description								
<i>enable</i>	Enable auto ASIC offloading.								
<i>disable</i>	Disable ASIC offloading.								

Parameter	Description	Type	Size
destination	Destination IP address of the tunnel.	ipv4-address	Not Specified
interface	Interface name.	string	Maximum length: 15
ip6	IPv6 address of the tunnel.	ipv6-prefix	Not Specified
name	Tunnel name.	string	Maximum length: 15
source	Source IP address of the tunnel.	ipv4-address	Not Specified

* This parameter may not exist in some models.

config system smc-ntp



This command is available for model(s): FortiGate 1100E, FortiGate 1101E, FortiGate 300E, FortiGate 301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 400D, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure SMC NTP information.

```
config system smc-ntp
    Description: Configure SMC NTP information.
    set channel {integer}
```

```

config ntpserver
    Description: Configure the FortiGate SMC to connect to an NTP server.
    edit <id>
        set server {ipv4-address}
    next
end
set ntpsync [enable|disable]
set syncinterval {integer}
end

```

config system smc-ntp

Parameter	Description	Type	Size						
channel	SMC NTP client will send NTP packets through this channel.	integer	Minimum value: 1 Maximum value: 65535						
ntpsync	Enable/disable setting the FortiGate SMC system time by synchronizing with an NTP server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with NTP server in SMC.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with NTP server in SMC.</td></tr></table>			Option	Description	<i>enable</i>	Enable synchronization with NTP server in SMC.	<i>disable</i>	Disable synchronization with NTP server in SMC.
Option	Description								
<i>enable</i>	Enable synchronization with NTP server in SMC.								
<i>disable</i>	Disable synchronization with NTP server in SMC.								
syncinterval	SMC NTP synchronization interval (1 - 65535 secs).	integer	Minimum value: 1 Maximum value: 65535						

config ntpserver

Parameter	Description	Type	Size
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295
server	IP address of the NTP server.	ipv4-address	Not Specified

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
name	Name of SMS server.	string	Maximum length: 35

config system snmp community

SNMP community configuration.

```

config system snmp community
    Description: SNMP community configuration.
    edit <id>
        set events {option1}, {option2}, ...
        config hosts
            Description: Configure IPv4 SNMP managers (hosts).
            edit <id>
                set ha-direct [enable|disable]
                set host-type [any|query|...]
                set ip {user}
                set source-ip {ipv4-address}
            next
        end
        config hosts6
            Description: Configure IPv6 SNMP managers.
            edit <id>
                set ha-direct [enable|disable]
                set host-type [any|query|...]
                set ipv6 {ipv6-prefix}
                set source-ipv6 {ipv6-address}
            next
        end
        set name {string}
        set query-v1-port {integer}
        set query-v1-status [enable|disable]
        set query-v2c-port {integer}
        set query-v2c-status [enable|disable]
        set status [enable|disable]
        set trap-v1-lport {integer}
        set trap-v1-rport {integer}
    end
end

```

```

set trap-v1-status [enable|disable]
set trap-v2c-lport {integer}
set trap-v2c-rport {integer}
set trap-v2c-status [enable|disable]
next
end

```

config system snmp community

Parameter	Description	Type	Size
events	SNMP trap events.	option	-

Option	Description
<i>cpu-high</i>	Send a trap when CPU usage is high.
<i>mem-low</i>	Send a trap when available memory is low.
<i>log-full</i>	Send a trap when log disk space becomes low.
<i>intf-ip</i>	Send a trap when an interface IP address is changed.
<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.
<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.
<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.
<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.
<i>ips-signature</i>	Send a trap when IPS detects an attack.
<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.
<i>av-virus</i>	Send a trap when AntiVirus finds a virus.
<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.
<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.
<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.
<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.
<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.
<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.

Parameter	Description	Type	Size

Option	Description
<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).
<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.
<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.
<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.
<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.
<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.
<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.
<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.
<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.
<i>power-supply-failure</i>	Send a trap when a power supply fails.
<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.
<i>fan-failure</i>	Send a trap when a fan fails.
<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.
<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.
<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.
<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.
<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.
<i>device-new</i>	Send a trap when a new device is found.
<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.

Parameter	Description	Type	Size						
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295						
name	Community name.	string	Maximum length: 35						
query-v1-port	SNMP v1 query port (default = 161).	integer	Minimum value: 1 Maximum value: 65535						
query-v1-status	Enable/disable SNMP v1 queries.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
query-v2c-port	SNMP v2c query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
status	Enable/disable this SNMP community.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
trap-v1-lport	SNMP v1 trap local port (default = 162).	integer	Minimum value: 1 Maximum value: 65535						

Parameter	Description	Type	Size
trap-v1-rport	SNMP v1 trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535
trap-v1-status	Enable/disable SNMP v1 traps.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
trap-v2c-lport	SNMP v2c trap local port (default = 162).	integer	Minimum value: 1 Maximum value: 65535
trap-v2c-rport	SNMP v2c trap remote port (default = 162).	integer	Minimum value: 1 Maximum value: 65535
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config hosts

Parameter	Description	Type	Size						
ha-direct	Enable/disable direct management of HA cluster members.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept queries from and send traps to this SNMP manager.</td></tr></table>			Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.		
Option	Description								
<i>any</i>	Accept queries from and send traps to this SNMP manager.								

Parameter	Description	Type	Size
	Option	Description	
	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.	
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IPv4 address of the SNMP manager (host).	user	Not Specified
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified

config hosts6

Parameter	Description	Type	Size								
ha-direct	Enable/disable direct management of HA cluster members.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept queries from and send traps to this SNMP manager.</td></tr><tr><td><i>query</i></td><td>Accept queries from this SNMP manager but do not send traps.</td></tr><tr><td><i>trap</i></td><td>Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.</td></tr></table>			Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.	<i>query</i>	Accept queries from this SNMP manager but do not send traps.	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.
Option	Description										
<i>any</i>	Accept queries from and send traps to this SNMP manager.										
<i>query</i>	Accept queries from this SNMP manager but do not send traps.										
<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.										
id	Host6 entry ID.	integer	Minimum value: 0 Maximum value: 4294967295								
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified								
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified								

config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
    Description: SNMP system info configuration.
    set contact-info {var-string}
    set description {var-string}
    set engine-id {string}
    set location {var-string}
    set status [enable|disable]
    set trap-high-cpu-threshold {integer}
    set trap-log-full-threshold {integer}
    set trap-low-memory-threshold {integer}
end
```

config system snmp sysinfo

Parameter	Description	Type	Size
contact-info	Contact information.	var-string	Maximum length: 255
description	System description.	var-string	Maximum length: 255
engine-id	Local SNMP engineID string (maximum 24 characters).	string	Maximum length: 24
location	System location.	var-string	Maximum length: 255
status	Enable/disable SNMP.	option	-
		Option	Description
		<i>enable</i>	Enable setting.
		<i>disable</i>	Disable setting.
trap-high-cpu-threshold	CPU 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
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100

config system snmp user

SNMP user configuration.

```
config system snmp user
  Description: SNMP user configuration.
  edit <name>
    set auth-proto [md5|sha|...]
    set auth-pwd {password}
    set events {option1}, {option2}, ...
    set ha-direct [enable|disable]
    set notify-hosts {ipv4-address}
    set notify-hosts6 {ipv6-address}
    set priv-proto [aes|des|...]
    set priv-pwd {password}
    set queries [enable|disable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
    set source-ip {ipv4-address}
    set source-ipv6 {ipv6-address}
    set status [enable|disable]
    set trap-lport {integer}
    set trap-rport {integer}
    set trap-status [enable|disable]
  next
end
```

config system snmp user

Parameter	Description	Type	Size
auth-proto	Authentication protocol.	option	-
	Option	Description	
	<i>md5</i>	HMAC-MD5-96 authentication protocol.	
	<i>sha</i>	HMAC-SHA-96 authentication protocol.	
	<i>sha224</i>	HMAC-SHA224 authentication protocol.	
	<i>sha256</i>	HMAC-SHA256 authentication protocol.	
	<i>sha384</i>	HMAC-SHA384 authentication protocol.	
	<i>sha512</i>	HMAC-SHA512 authentication protocol.	
auth-pwd	Password for authentication protocol.	password	Not Specified
events	SNMP notifications (traps) to send.	option	-

Parameter	Description	Type	Size

Option	Description
<i>cpu-high</i>	Send a trap when CPU usage is high.
<i>mem-low</i>	Send a trap when available memory is low.
<i>log-full</i>	Send a trap when log disk space becomes low.
<i>intf-ip</i>	Send a trap when an interface IP address is changed.
<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.
<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.
<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.
<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.
<i>ips-signature</i>	Send a trap when IPS detects an attack.
<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.
<i>av-virus</i>	Send a trap when AntiVirus finds a virus.
<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.
<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.
<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.
<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.
<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.
<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.
<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).
<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.
<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.
<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.
<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.

Parameter	Description	Type	Size

Option	Description
<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.
<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.
<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.
<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.
<i>power-supply-failure</i>	Send a trap when a power supply fails.
<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.
<i>fan-failure</i>	Send a trap when a fan fails.
<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.
<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.
<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.
<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.
<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.
<i>device-new</i>	Send a trap when a new device is found.
<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.

ha-direct	Enable/disable direct management of HA cluster members.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

name	SNMP user name.	string	Maximum length: 32
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified
priv-proto	Privacy (encryption) protocol.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.	
	<i>des</i>	CBC-DES symmetric encryption protocol.	
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.	
	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.	
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified
queries	Enable/disable SNMP queries for this user.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
query-port	SNMPv3 query port (default = 161).	integer	Minimum value: 0 Maximum value: 65535
security-level	Security level for message authentication and encryption.	option	-
	Option	Description	
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	
	<i>auth-priv</i>	Message with authentication and privacy (encryption).	
source-ip	Source IP for SNMP trap.	ipv4-address	Not Specified
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified
status	Enable/disable this SNMP user.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
trap-lport	SNMPv3 local trap port (default = 162).	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
trap-rport	SNMPv3 trap remote port (default = 162).	integer	Minimum value: 0 Maximum value: 65535
trap-status	Enable/disable traps for this SNMP user.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config system speed-test-server



The `config system speed-test-server` command is read-only. Administrators cannot configure custom servers.

Configure speed test server list.

```
config system speed-test-server
  Description: Configure speed test server list.
  edit <name>
    config host
      Description: Hosts of the server.
      edit <id>
        set ip {ipv4-address}
        set password {password}
        set port {integer}
        set user {string}
      next
    end
    set timestamp {integer}
  next
end
```

config system speed-test-server

Parameter	Description	Type	Size
name	Speed test server name.	string	Maximum length: 35

Parameter	Description	Type	Size
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295

config host

Parameter	Description	Type	Size
id	Server host ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	Server host IPv4 address.	ipv4-address	Not Specified
password	Speed test host password.	password	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

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

Parameter	Description	Type	Size
name	SSO admin name.	string	Maximum length: 64
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79

config system storage

Configure logical storage.

```
config system storage
    Description: Configure logical storage.
    edit <name>
        set device {string}
        set media-status [enable|disable|...]
        set order {integer}
        set partition {string}
        set size {integer}
        set status [enable|disable]
        set usage [log|wanopt]
        set wanopt-mode [mix|wanopt|...]
    next
end
```

config system storage

Parameter	Description	Type	Size
device	Partition device.	string	Maximum length: 19
media-status	The physical status of current media.	option	-
	Option	Description	
	enable	Storage is enabled.	
	disable	Storage is disabled.	
	fail	Storage have some fail sector.	
name	Storage name.	string	Maximum length: 35
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255

Parameter	Description	Type	Size								
partition	Label of underlying partition.	string	Maximum length: 16								
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295								
status	Enable/disable storage.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
usage	Use hard disk for logging or WAN Optimization (default = log).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>log</i></td><td>Use hard disk for logging.</td></tr><tr><td><i>wanopt</i></td><td>Use hard disk for WAN Optimization.</td></tr></table>	Option	Description	<i>log</i>	Use hard disk for logging.	<i>wanopt</i>	Use hard disk for WAN Optimization.				
Option	Description										
<i>log</i>	Use hard disk for logging.										
<i>wanopt</i>	Use hard disk for WAN Optimization.										
wanopt-mode *	WAN Optimization mode (default = mix).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mix</i></td><td>Use hard disk for WAN Optimization mix mode.</td></tr><tr><td><i>wanopt</i></td><td>Use hard disk for WAN Optimization wanopt mode.</td></tr><tr><td><i>webcache</i></td><td>Use hard disk for WAN Optimization webcache mode.</td></tr></table>	Option	Description	<i>mix</i>	Use hard disk for WAN Optimization mix mode.	<i>wanopt</i>	Use hard disk for WAN Optimization wanopt mode.	<i>webcache</i>	Use hard disk for WAN Optimization webcache mode.		
Option	Description										
<i>mix</i>	Use hard disk for WAN Optimization mix mode.										
<i>wanopt</i>	Use hard disk for WAN Optimization wanopt mode.										
<i>webcache</i>	Use hard disk for WAN Optimization webcache mode.										

* This parameter may not exist in some models.

config system stp



This command is available for model(s): FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3800D, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate 92D, FortiGate-VM64, FortiGateRugged 35D, FortiGateRugged 90D.

Configure Spanning Tree Protocol (STP).

```
config system stp
    Description: Configure Spanning Tree Protocol (STP).
    set forward-delay {integer}
    set hello-time {integer}
    set max-age {integer}
    set max-hops {integer}
    set switch-priority [0|4096|...]
end
```

config system stp

Parameter	Description	Type	Size
forward-delay	Forward delay (4 - 30 sec, default = 15).	integer	Minimum value: 4 Maximum value: 30

Parameter	Description	Type	Size
hello-time	Hello time (1 - 10 sec, default = 2).	integer	Minimum value: 1 Maximum value: 10
max-age	Maximum packet age (6 - 40 sec, default = 20).	integer	Minimum value: 6 Maximum value: 40
max-hops	Maximum number of hops (1 - 40, default = 20).	integer	Minimum value: 1 Maximum value: 40
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	-

Option	Description
0	0
4096	4096
8192	8192
12288	12288
16384	16384
20480	20480
24576	24576
28672	28672
32768	32768
36864	36864
40960	40960
45056	45056
49152	49152
53248	53248
57344	57344

config system switch-interface

Configure software switch interfaces by grouping physical and WiFi interfaces.

```

config system switch-interface
    Description: Configure software switch interfaces by grouping physical and WiFi
    interfaces.
    edit <name>
        set intra-switch-policy [implicit|explicit]
        set member <interface-name1>, <interface-name2>, ...
        set span [disable|enable]
        set span-dest-port {string}
        set span-direction [rx|tx|...]
        set span-source-port <interface-name1>, <interface-name2>, ...
        set type [switch|hub]
        set vdom {string}
    next
end

```

config system switch-interface

Parameter	Description	Type	Size
intra-switch-policy	Allow any traffic between switch interfaces or require firewall policies to allow traffic between switch interfaces.	option	-
	Option	Description	
	<i>implicit</i>	Traffic between switch members is implicitly allowed.	
	<i>explicit</i>	Traffic between switch members must match firewall policies.	
member <interface-name>	Names of the interfaces that belong to the virtual switch. Physical interface name.	string	Maximum length: 79
name	Interface name (name cannot be in use by any other interfaces, VLANs, or inter-VDOM links).	string	Maximum length: 15
span	Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span destination port.	option	-
	Option	Description	
	<i>disable</i>	Disable port spanning.	
	<i>enable</i>	Enable port spanning.	
span-dest-port	SPAN destination port name. All traffic on the SPAN source ports is echoed to the SPAN destination port.	string	Maximum length: 15
span-direction	The direction in which the SPAN port operates, either: rx, tx, or both.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rx</i></td><td>Copies only received packets from source SPAN ports to the destination SPAN port.</td></tr><tr><td><i>tx</i></td><td>Copies only transmitted packets from source SPAN ports to the destination SPAN port.</td></tr><tr><td><i>both</i></td><td>Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.</td></tr></table>	Option	Description	<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.	<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.	<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.		
	Option	Description									
	<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.									
	<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.									
<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.										
span-source-port <interface-name>	Physical interface name. Port spanning echoes all traffic on the SPAN source ports to the SPAN destination port. Physical interface name.	string	Maximum length: 79								
type	Type of switch based on functionality: switch for normal functionality, or hub to duplicate packets to all port members.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>switch</i></td><td>Switch for normal switch functionality (available in NAT mode only).</td></tr><tr><td><i>hub</i></td><td>Hub to duplicate packets to all member ports.</td></tr></table>	Option	Description	<i>switch</i>	Switch for normal switch functionality (available in NAT mode only).	<i>hub</i>	Hub to duplicate packets to all member ports.				
	Option	Description									
	<i>switch</i>	Switch for normal switch functionality (available in NAT mode only).									
<i>hub</i>	Hub to duplicate packets to all member ports.										
vdom	VDOM that the software switch belongs to.	string	Maximum length: 31								

config system tos-based-priority

Configure Type of Service (ToS) based priority table to set network traffic priorities.

```

config system tos-based-priority
    Description: Configure Type of Service (ToS) based priority table to set network traffic
priorities.
    edit <id>
        set priority [low|medium|...]
        set tos {integer}
    next
end

```

config system tos-based-priority

Parameter	Description	Type	Size								
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295								
priority	ToS based priority level to low, medium or high (these priorities match firewall traffic shaping priorities) (default = medium).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Low priority.</td></tr><tr><td><i>medium</i></td><td>Medium priority.</td></tr><tr><td><i>high</i></td><td>High priority.</td></tr></table>	Option	Description	<i>low</i>	Low priority.	<i>medium</i>	Medium priority.	<i>high</i>	High priority.		
Option	Description										
<i>low</i>	Low priority.										
<i>medium</i>	Medium priority.										
<i>high</i>	High priority.										
tos	Value of the ToS byte in the IP datagram header (0-15, 8: minimize delay, 4: maximize throughput, 2: maximize reliability, 1: minimize monetary cost, and 0: default service).	integer	Minimum value: 0 Maximum value: 15								

config system vdom

Configure virtual domain.

```
config system vdom
  Description: Configure virtual domain.
  edit <name>
    set flag {integer}
    set short-name {string}
    set vcluster-id {integer}
  next
end
```

config system vdom

Parameter	Description	Type	Size
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
name	VDOM name.	string	Maximum length: 31
short-name	VDOM short name.	string	Maximum length: 11
vcluster-id	Virtual cluster ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295

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 dns-over-tls [disable|enable|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set primary {ipv4-address}
    set secondary {ipv4-address}
    set server-hostname <hostname1>, <hostname2>, ...
    set source-ip {ipv4-address}
    set ssl-certificate {string}
    set vdom-dns [enable|disable]
end

```

config system vdom-dns

Parameter	Description	Type	Size
dns-over-tls	Enable/disable/enforce DNS over TLS.	option	-
	Option	Description	
	<i>disable</i>	Disable DNS over TLS.	
	<i>enable</i>	Use TLS for DNS queries if TLS is available.	
	<i>enforce</i>	Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15

Parameter	Description	Type	Size								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.		
	Option	Description									
	auto	Set outgoing interface automatically.									
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.									
specify	Set outgoing interface manually.										
ip6-primary	Primary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified								
ip6-secondary	Secondary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified								
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified								
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified								
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127								
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified								
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35								
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable configuring DNS servers for the current VDOM.</td></tr><tr><td>disable</td><td>Disable configuring DNS servers for the current VDOM.</td></tr></table>	Option	Description	enable	Enable configuring DNS servers for the current VDOM.	disable	Disable configuring DNS servers for the current VDOM.				
	Option	Description									
	enable	Enable configuring DNS servers for the current VDOM.									
disable	Disable configuring DNS servers for the current VDOM.										

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
id	Index <1-4096>.	integer	Minimum value: 0 Maximum value: 4294967295
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-

Option	Description
<i>log.fortianalyzer.setting</i>	log.fortianalyzer.setting
<i>log.fortianalyzer.override-setting</i>	log.fortianalyzer.override-setting
<i>log.fortianalyzer2.setting</i>	log.fortianalyzer2.setting
<i>log.fortianalyzer2.override-setting</i>	log.fortianalyzer2.override-setting
<i>log.fortianalyzer3.setting</i>	log.fortianalyzer3.setting
<i>log.fortianalyzer3.override-setting</i>	log.fortianalyzer3.override-setting
<i>log.fortianalyzer-cloud.setting</i>	log.fortianalyzer-cloud.setting
<i>log.fortianalyzer-cloud.override-setting</i>	log.fortianalyzer-cloud.override-setting
<i>system.central-management</i>	system.central-management
<i>system.csf</i>	system.csf
<i>user.radius</i>	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
<i>all</i>	Object configuration independent for all VDOMs.

Parameter	Description	Type	Size
	Option	Description	
	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.	
	<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.	
vdom <name>	Names of the VDOMs. VDOM name.	string	Maximum length: 79

config system vdom-link

Configure VDOM links.

```
config system vdom-link
    Description: Configure VDOM links.
    edit <name>
        set type [ppp|ethernet]
        set vcluster [vcluster1|vcluster2]
    next
end
```

config system vdom-link

Parameter	Description	Type	Size
name	VDOM link name (maximum = 8 characters).	string	Maximum length: 11
type	VDOM link type: PPP or Ethernet.	option	-
	Option	Description	
	<i>ppp</i>	PPP VDOM link.	
	<i>ethernet</i>	Ethernet VDOM link.	
vcluster	Virtual cluster.	option	-
	Option	Description	
	<i>vcluster1</i>	Virtual cluster 1.	
	<i>vcluster2</i>	Virtual cluster 2.	

config system vdom-netflow

Configure NetFlow per VDOM.

```
config system vdom-netflow
  Description: Configure NetFlow per VDOM.
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set source-ip {ipv4-address}
  set vdom-netflow [enable|disable]
end
```

config system vdom-netflow

Parameter	Description	Type	Size
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
vdom-netflow	Enable/disable NetFlow per VDOM.	option	-
		Option	Description
		<i>enable</i>	Enable NetFlow per VDOM.
		<i>disable</i>	Disable NetFlow per VDOM.

config system vdom-property

Configure VDOM property.

```
config system vdom-property
  Description: Configure VDOM property.
  edit <name>
    set custom-service {user}
    set description {string}
    set dialup-tunnel {user}
    set firewall-address {user}
    set firewall-addrgrp {user}
    set firewall-policy {user}
    set ipsec-phase1 {user}
    set ipsec-phase1-interface {user}
    set ipsec-phase2 {user}
    set ipsec-phase2-interface {user}
    set log-disk-quota {user}
  end
```

```

        set onetime-schedule {user}
        set proxy {user}
        set recurring-schedule {user}
        set service-group {user}
        set session {user}
        set snmp-index {integer}
        set sslvpn {user}
        set user {user}
        set user-group {user}
    next
end

```

config system vdom-property

Parameter	Description	Type	Size
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified
description	Description.	string	Maximum length: 127
dialup-tunnel	Maximum guaranteed number of dial-up tunnels.	user	Not Specified
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified
firewall-addgrp	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified
firewall-policy	Maximum guaranteed number of firewall policies (IPv4, IPv6, policy46, policy64, DoS-policy4, DoS-policy6, multicast).	user	Not Specified
ipsec-phase1	Maximum guaranteed number of VPN IPsec phase 1 tunnels.	user	Not Specified
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified
ipsec-phase2	Maximum guaranteed number of VPN IPsec phase 2 tunnels.	user	Not Specified
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified
log-disk-quota	Log disk quota in MB (range depends on how much disk space is available).	user	Not Specified
name	VDOM name.	string	Maximum length: 31
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified

Parameter	Description	Type	Size
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified
session	Maximum guaranteed number of sessions.	user	Not Specified
snmp-index	Permanent SNMP Index of the virtual domain (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
sslvpn	Maximum guaranteed number of SSL-VPNs.	user	Not Specified
user	Maximum guaranteed number of local users.	user	Not Specified
user-group	Maximum guaranteed number of user groups.	user	Not Specified

config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
    Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server
for this VDOM.
    edit <name>
        set radius-server-vdom {string}
        set status [enable|disable]
    next
end
```

config system vdom-radius-server

Parameter	Description	Type	Size
name	Name of the VDOM that you are adding the RADIUS server to.	string	Maximum length: 31
radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-

Option	Description
<i>enable</i>	Enable the RSSO RADIUS server for this VDOM.
<i>disable</i>	Disable the RSSO RADIUS server for this VDOM.

config system vdom-sflow

Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.

```
config system vdom-sflow
    Description: Configure sFlow per VDOM to add or change the IP address and UDP port that
FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.
    set collector-ip {ipv4-address}
    set collector-port {integer}
    set source-ip {ipv4-address}
    set vdom-sflow [enable|disable]
end
```

config system vdom-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 (default = 0.0.0.0).	ipv4-address	Not Specified
collector-port	UDP port number used for sending sFlow datagrams (configure only if required by your sFlow collector or your network configuration) (0 - 65535, default = 6343).	integer	Minimum value: 0 Maximum value: 65535
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified
vdom-sflow	Enable/disable the sFlow configuration for the current VDOM.	option	-

Option	Description
<i>enable</i>	Enable sFlow for this VDOM.
<i>disable</i>	Disable sFlow for this VDOM.

config system virtual-switch



This command is available for model(s): FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3800D, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGateRugged 30D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate-VM64, FortiGateRugged 35D, FortiGateRugged 90D.

Configure virtual hardware switch interfaces.

```
config system virtual-switch
  Description: Configure virtual hardware switch interfaces.
  edit <name>
    set physical-switch {string}
    config port
      Description: Configure member ports.
      edit <name>
        set alias {string}
        set speed [auto|10full|...]
        set status [up|down]
      next
    end
    set qos [none|802.1p]
    set span [disable|enable]
    set span-dest-port {string}
    set span-direction [rx|tx|...]
    set span-source-port {string}
    set vlan {integer}
  next
end
```

config system virtual-switch

Parameter	Description	Type	Size								
name	Name of the virtual switch.	string	Maximum length: 15								
physical-switch	Physical switch parent.	string	Maximum length: 15								
qos *	set QOS none or 8021p	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable QOS</td></tr><tr><td><i>802.1p</i></td><td>Enable QOS 802.1p</td></tr></table>	Option	Description	<i>none</i>	Disable QOS	<i>802.1p</i>	Enable QOS 802.1p				
Option	Description										
<i>none</i>	Disable QOS										
<i>802.1p</i>	Enable QOS 802.1p										
span	Enable/disable SPAN.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SPAN.</td></tr><tr><td><i>enable</i></td><td>Enable SPAN.</td></tr></table>	Option	Description	<i>disable</i>	Disable SPAN.	<i>enable</i>	Enable SPAN.				
Option	Description										
<i>disable</i>	Disable SPAN.										
<i>enable</i>	Enable SPAN.										
span-dest-port	SPAN destination port.	string	Maximum length: 15								
span-direction	SPAN direction.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rx</i></td><td>Span receive direction only.</td></tr><tr><td><i>tx</i></td><td>Span transmit direction only.</td></tr><tr><td><i>both</i></td><td>Span both directions.</td></tr></table>	Option	Description	<i>rx</i>	Span receive direction only.	<i>tx</i>	Span transmit direction only.	<i>both</i>	Span both directions.		
Option	Description										
<i>rx</i>	Span receive direction only.										
<i>tx</i>	Span transmit direction only.										
<i>both</i>	Span both directions.										
span-source-port	SPAN source ports.	string	Maximum length: 15								
vlan *	VLAN.	integer	Minimum value: 0 Maximum value: 4294967295								

* This parameter may not exist in some models.

config port

Parameter	Description	Type	Size
alias	Alias.	string	Maximum length: 25
name	Physical interface name.	string	Maximum length: 15
speed	Interface speed.	option	-

Option	Description
<i>auto</i>	Automatically adjust speed.
<i>10full</i>	10M full-duplex.
<i>10half</i>	10M half-duplex.
<i>100full</i>	100M full-duplex.
<i>100half</i>	100M half-duplex.
<i>1000full</i>	1000M full-duplex.
<i>1000half</i>	1000M half-duplex.
<i>1000auto</i>	1000M auto adjust.

status	Interface status.	option	-

Option	Description
<i>up</i>	Interface up.
<i>down</i>	Interface down.

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 fail-alert-interfaces <name1>, <name2>, ...
    set fail-detect [enable|disable]
    config health-check
        Description: SD-WAN status checking or health checking. Identify a server on the Internet and determine how SD-WAN verifies that the FortiGate can communicate with it.
        edit <name>
            set addr-mode [ipv4|ipv6]
            set diffservcode {user}
            set failtime {integer}
            set ha-priority {integer}
            set http-agent {string}
```

```

set http-get {string}
set http-match {string}
set interval {integer}
set members <seq-num1>, <seq-num2>, ...
set packet-size {integer}
set password {password}
set port {integer}
set probe-packets [disable|enable]
set probe-timeout {integer}
set protocol [ping|tcp-echo|...]
set recoverytime {integer}
set security-mode [none|authentication]
set server {string}
config sla
    Description: Service level agreement (SLA).
    edit <id>
        set jitter-threshold {integer}
        set latency-threshold {integer}
        set link-cost-factor {option1}, {option2}, ...
        set packetloss-threshold {integer}
    next
end
set sla-fail-log-period {integer}
set sla-pass-log-period {integer}
set threshold-alert-jitter {integer}
set threshold-alert-latency {integer}
set threshold-alert-packetloss {integer}
set threshold-warning-jitter {integer}
set threshold-warning-latency {integer}
set threshold-warning-packetloss {integer}
set update-cascade-interface [enable|disable]
set update-static-route [enable|disable]
next
end
set load-balance-mode [source-ip-based|weight-based|...]
config members
    Description: FortiGate interfaces added to the virtual-wan-link.
    edit <seq-num>
        set comment {var-string}
        set cost {integer}
        set gateway {ipv4-address}
        set gateway6 {ipv6-address}
        set ingress-spillover-threshold {integer}
        set interface {string}
        set priority {integer}
        set source {ipv4-address}
        set source6 {ipv6-address}
        set spillover-threshold {integer}
        set status [disable|enable]
        set volume-ratio {integer}
        set weight {integer}
    next
end
config neighbor
    Description: Create SD-WAN neighbor from BGP neighbor table to control route
    advertisements according to SLA status.

```

```

edit <ip>
    set health-check {string}
    set member {integer}
    set role [standalone|primary|...]
    set sla-id {integer}
next
end
set neighbor-hold-boot-time {integer}
set neighbor-hold-down [enable|disable]
set neighbor-hold-down-time {integer}
config service
    Description: Create SD-WAN rules (also called services) to control how sessions are
distributed to interfaces in the SD-WAN.
    edit <id>
        set addr-mode [ipv4|ipv6]
        set bandwidth-weight {integer}
        set default [enable|disable]
        set dscp-forward [enable|disable]
        set dscp-forward-tag {user}
        set dscp-reverse [enable|disable]
        set dscp-reverse-tag {user}
        set dst <name1>, <name2>, ...
        set dst-negate [enable|disable]
        set dst6 <name1>, <name2>, ...
        set end-port {integer}
        set gateway [enable|disable]
        set groups <name1>, <name2>, ...
        set health-check {string}
        set hold-down-time {integer}
        set input-device <name1>, <name2>, ...
        set input-device-negate [enable|disable]
        set internet-service [enable|disable]
        set internet-service-app-ctrl <id1>, <id2>, ...
        set internet-service-app-ctrl-group <name1>, <name2>, ...
        set internet-service-custom <name1>, <name2>, ...
        set internet-service-custom-group <name1>, <name2>, ...
        set internet-service-group <name1>, <name2>, ...
        set internet-service-id <id1>, <id2>, ...
        set jitter-weight {integer}
        set latency-weight {integer}
        set link-cost-factor [latency|jitter|...]
        set link-cost-threshold {integer}
        set mode [auto|manual|...]
        set name {string}
        set packet-loss-weight {integer}
        set priority-members <seq-num1>, <seq-num2>, ...
        set protocol {integer}
        set quality-link {integer}
        set role [standalone|primary|...]
        set route-tag {integer}
    config sla
        Description: Service level agreement (SLA).
        edit <health-check>
            set id {integer}
        next
    end
end

```

```

        set sla-compare-method [order|number]
        set src <name1>, <name2>, ...
        set src-negate [enable|disable]
        set src6 <name1>, <name2>, ...
        set standalone-action [enable|disable]
        set start-port {integer}
        set status [enable|disable]
        set tos {user}
        set tos-mask {user}
        set users <name1>, <name2>, ...
    next
end
set status [disable|enable]
config zone
    Description: Configure SD-WAN zones.
    edit <name>
    next
end
end

```

config system virtual-wan-link

Parameter	Description	Type	Size										
fail-alert-interfaces <name>	Physical interfaces that will be alerted. Physical interface name.	string	Maximum length: 79										
fail-detect	Enable/disable SD-WAN Internet connection status checking (failure detection).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable status checking.</td></tr><tr><td>disable</td><td>Disable status checking.</td></tr></table>			Option	Description	enable	Enable status checking.	disable	Disable status checking.				
Option	Description												
enable	Enable status checking.												
disable	Disable status checking.												
load-balance-mode	Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>source-ip-based</td><td>Source IP load balancing. All traffic from a source IP is sent to the same interface.</td></tr><tr><td>weight-based</td><td>Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.</td></tr><tr><td>usage-based</td><td>Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.</td></tr><tr><td>source-dest-ip-based</td><td>Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.</td></tr></table>			Option	Description	source-ip-based	Source IP load balancing. All traffic from a source IP is sent to the same interface.	weight-based	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.	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.
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.												

Parameter	Description	Type	Size
	Option	Description	
	<i>measured-volume-based</i>	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.	
neighbor-hold-boot-time	Waiting period in seconds when switching from the primary neighbor to the secondary neighbor from the neighbor start. (0 - 10000000, default = 0).	integer	Minimum value: 0 Maximum value: 10000000
neighbor-hold-down	Enable/disable hold switching from the secondary neighbor to the primary neighbor.	option	-
	Option	Description	
	<i>enable</i>	Enable hold switching from the secondary neighbor to the primary neighbor.	
	<i>disable</i>	Disable hold switching from the secondary neighbor to the primary neighbor.	
neighbor-hold-down-time	Waiting period in seconds when switching from the secondary neighbor to the primary neighbor when hold-down is disabled. (0 - 10000000, default = 0).	integer	Minimum value: 0 Maximum value: 10000000
status	Enable/disable SD-WAN.	option	-
	Option	Description	
	<i>disable</i>	Disable SD-WAN.	
	<i>enable</i>	Enable SD-WAN.	

config health-check

Parameter	Description	Type	Size
addr-mode	Address mode (IPv4 or IPv6).	option	-
	Option	Description	
	<i>ipv4</i>	IPv4 mode.	
	<i>ipv6</i>	IPv6 mode.	
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified

Parameter	Description	Type	Size
failtime	Number of failures before server is considered lost (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600
ha-priority	HA election priority (1 - 50).	integer	Minimum value: 1 Maximum value: 50
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024
http-get	URL used to communicate with the server if the protocol is HTTP.	string	Maximum length: 1024
http-match	Response string expected from the server if the protocol is HTTP.	string	Maximum length: 1024
interval	Status check interval in milliseconds, or the time between attempting to connect to the server (500 - 3600*1000 msec, default = 500).	integer	Minimum value: 500 Maximum value: 3600000
members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295
name	Status check or health check name.	string	Maximum length: 35
packet-size	Packet size of a twamp test session,	integer	Minimum value: 64 Maximum value: 1024
password	Twamp controller password in authentication mode	password	Not Specified
port	Port number used to communicate with the server over the selected protocol.	integer	Minimum value: 1 Maximum value: 65535
probe-packets	Enable/disable transmission of probe packets.	option	-

Option	Description
<i>disable</i>	Disable transmission of probe packets.
<i>enable</i>	Enable transmission of probe packets.

Parameter	Description	Type	Size
probe-timeout	Time to wait before a probe packet is considered lost (500 - 5000 msec, default = 500).	integer	Minimum value: 500 Maximum value: 5000
protocol	Protocol used to determine if the FortiGate can communicate with the server.	option	-
	Option	Description	
	<i>ping</i>	Use PING to test the link with the server.	
	<i>tcp-echo</i>	Use TCP echo to test the link with the server.	
	<i>udp-echo</i>	Use UDP echo to test the link with the server.	
	<i>http</i>	Use HTTP-GET to test the link with the server.	
	<i>twamp</i>	Use TWAMP to test the link with the server.	
	<i>ping6</i>	PING6 link monitor.	
recoverytime	Number of successful responses received before server is considered recovered (1 - 3600, default = 5).	integer	Minimum value: 1 Maximum value: 3600
security-mode	Twamp controller security mode.	option	-
	Option	Description	
	<i>none</i>	Unauthenticated mode.	
	<i>authentication</i>	Authenticated mode.	
server	IP address or FQDN name of the server.	string	Maximum length: 79
sla-fail-log-period	Time interval in seconds that SLA fail log messages will be generated (0 - 3600, default = 0).	integer	Minimum value: 0 Maximum value: 3600
sla-pass-log-period	Time interval in seconds that SLA pass log messages will be generated (0 - 3600, default = 0).	integer	Minimum value: 0 Maximum value: 3600
threshold-alert-jitter	Alert threshold for jitter (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
threshold-alert-latency	Alert threshold for latency (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295
threshold-alert-packetloss	Alert threshold for packet loss (percentage, default = 0).	integer	Minimum value: 0 Maximum value: 100
threshold-warning-jitter	Warning threshold for jitter (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295
threshold-warning-latency	Warning threshold for latency (ms, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295
threshold-warning-packetloss	Warning threshold for packet loss (percentage, default = 0).	integer	Minimum value: 0 Maximum value: 100
update-cascade-interface	Enable/disable update cascade interface.	option	-

Option	Description
<i>enable</i>	Enable update cascade interface.
<i>disable</i>	Disable update cascade interface.

update-static-route	Enable/disable updating the static route.	option	-

Option	Description
<i>enable</i>	Enable updating the static route.
<i>disable</i>	Disable updating the static route.

config sla

Parameter	Description	Type	Size								
id	SLA ID.	integer	Minimum value: 1 Maximum value: 32								
jitter-threshold	Jitter for SLA to make decision in milliseconds. (0 - 10000000, default = 5).	integer	Minimum value: 0 Maximum value: 10000000								
latency-threshold	Latency for SLA to make decision in milliseconds. (0 - 10000000, default = 5).	integer	Minimum value: 0 Maximum value: 10000000								
link-cost-factor	Criteria on which to base link selection.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>latency</i></td><td>Select link based on latency.</td></tr><tr><td><i>jitter</i></td><td>Select link based on jitter.</td></tr><tr><td><i>packet-loss</i></td><td>Select link based on packet loss.</td></tr></table>		Option	Description	<i>latency</i>	Select link based on latency.	<i>jitter</i>	Select link based on jitter.	<i>packet-loss</i>	Select link based on packet loss.	
	Option	Description									
	<i>latency</i>	Select link based on latency.									
	<i>jitter</i>	Select link based on jitter.									
<i>packet-loss</i>	Select link based on packet loss.										
packetloss-threshold	Packet loss for SLA to make decision in percentage. (0 - 100, default = 0).	integer	Minimum value: 0 Maximum value: 100								

config members

Parameter	Description	Type	Size
comment	Comments.	var-string	Maximum length: 255
cost	Cost of this interface for services in SLA mode (0 - 4294967295, default = 0).	integer	Minimum value: 0 Maximum value: 4294967295
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

Parameter	Description	Type	Size						
gateway6	IPv6 gateway.	ipv6-address	Not Specified						
ingress-spillover-threshold	Ingress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000						
interface	Interface name.	string	Maximum length: 15						
priority	Priority of the interface (0 - 4294967295). Used for SD-WAN rules or priority rules.	integer	Minimum value: 0 Maximum value: 4294967295						
seq-num	Sequence number(1-255).	integer	Minimum value: 0 Maximum value: 255						
source	Source IP address used in the health-check packet to the server.	ipv4-address	Not Specified						
source6	Source IPv6 address used in the health-check packet to the server.	ipv6-address	Not Specified						
spillover-threshold	Egress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000						
status	Enable/disable this interface in the SD-WAN.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable this interface in the SD-WAN.</td></tr><tr><td>enable</td><td>Enable this interface in the SD-WAN.</td></tr></table>			Option	Description	disable	Disable this interface in the SD-WAN.	enable	Enable this interface in the SD-WAN.
	Option	Description							
	disable	Disable this interface in the SD-WAN.							
enable	Enable this interface in the SD-WAN.								
volume-ratio	Measured volume ratio (this value / sum of all values = percentage of link volume, 1 - 255).	integer	Minimum value: 1 Maximum value: 255						
weight	Weight of this interface for weighted load balancing. (1 - 255) More traffic is directed to interfaces with higher weights.	integer	Minimum value: 1 Maximum value: 255						

config neighbor

Parameter	Description	Type	Size
health-check	SD-WAN health-check name.	string	Maximum length: 35
ip	IP address of neighbor.	string	Maximum length: 45
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.	
sla-id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295

config service

Parameter	Description	Type	Size
addr-mode	Address mode (IPv4 or IPv6).	option	-
	Option	Description	
	ipv4	IPv4 mode.	
	ipv6	IPv6 mode.	
bandwidth-weight	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
default	Enable/disable use of SD-WAN as default service.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable use of SD-WAN as default service.	
	<i>disable</i>	Disable use of SD-WAN as default service.	
dscp-forward	Enable/disable forward traffic DSCP tag.	option	-
	Option	Description	
	<i>enable</i>	Enable use of forward DSCP tag.	
	<i>disable</i>	Disable use of forward DSCP tag.	
dscp-forward-tag	Forward traffic DSCP tag.	user	Not Specified
dscp-reverse	Enable/disable reverse traffic DSCP tag.	option	-
	Option	Description	
	<i>enable</i>	Enable use of reverse DSCP tag.	
	<i>disable</i>	Disable use of reverse DSCP tag.	
dscp-reverse-tag	Reverse traffic DSCP tag.	user	Not Specified
dst <name>	Destination address name. Address or address group name.	string	Maximum length: 79
dst-negate	Enable/disable negation of destination address match.	option	-
	Option	Description	
	<i>enable</i>	Enable destination address negation.	
	<i>disable</i>	Disable destination address negation.	
dst6 <name>	Destination address6 name. Address6 or address6 group name.	string	Maximum length: 79
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535
gateway	Enable/disable SD-WAN service gateway.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable SD-WAN service gateway.	
	<i>disable</i>	Disable SD-WAN service gateway.	
groups <name>	User groups. Group name.	string	Maximum length: 79
health-check	Health check.	string	Maximum length: 35
hold-down-time	Waiting period in seconds when switching from the back-up member to the primary member (0 - 10000000, default = 0).	integer	Minimum value: 0 Maximum value: 10000000
id	Priority rule ID (1 - 4000).	integer	Minimum value: 1 Maximum value: 4000
input-device <name>	Source interface name. Interface name.	string	Maximum length: 79
input-device-negate	Enable/disable negation of input device match.	option	-
	Option	Description	
	<i>enable</i>	Enable negation of input device match.	
	<i>disable</i>	Disable negation of input device match.	
internet-service	Enable/disable use of Internet service for application-based load balancing.	option	-
	Option	Description	
	<i>enable</i>	Enable cloud service to support application-based load balancing.	
	<i>disable</i>	Disable cloud service to support application-based load balancing.	
internet-service-app-ctrl <id>	Application control based Internet Service ID list. Application control based Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
internet-service-app-ctrl-group <name>	Application control based Internet Service group list. Application control based Internet Service group name.	string	Maximum length: 79
internet-service-custom <name>	Custom Internet service name list. Custom Internet service name.	string	Maximum length: 79
internet-service-custom-group <name>	Custom Internet Service group list. Custom Internet Service group name.	string	Maximum length: 79
internet-service-group <name>	Internet Service group list. Internet Service group name.	string	Maximum length: 79
internet-service-id <id>	Internet service ID list. Internet service ID.	integer	Minimum value: 0 Maximum value: 4294967295
jitter-weight	Coefficient of jitter in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
latency-weight	Coefficient of latency in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
link-cost-factor	Link cost factor.	option	-

Option	Description
<i>latency</i>	Select link based on latency.
<i>jitter</i>	Select link based on jitter.
<i>packet-loss</i>	Select link based on packet loss.
<i>inbandwidth</i>	Select link based on available bandwidth of incoming traffic.
<i>outbandwidth</i>	Select link based on available bandwidth of outgoing traffic.
<i>bibandwidth</i>	Select link based on available bandwidth of bidirectional traffic.
<i>custom-profile-1</i>	Select link based on customized profile.

Parameter	Description	Type	Size
link-cost-threshold	Percentage threshold change of link cost values that will result in policy route regeneration (0 - 10000000, default = 10).	integer	Minimum value: 0 Maximum value: 10000000
mode	Control how the priority rule sets the priority of interfaces in the SD-WAN.	option	-

Option	Description
<i>auto</i>	Assign interfaces a priority based on quality.
<i>manual</i>	Assign interfaces a priority manually.
<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.
<i>sla</i>	Assign interfaces a priority based on selected SLA settings.
<i>load-balance</i>	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.

name	Priority rule name.	string	Maximum length: 35
packet-loss-weight	Coefficient of packet-loss in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000
priority-members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255
quality-link	Quality grade.	integer	Minimum value: 0 Maximum value: 255
role	Service role to work with neighbor.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>standalone</i>	Standalone service.	
	<i>primary</i>	Primary service for primary neighbor.	
	<i>secondary</i>	Secondary service for secondary neighbor.	
route-tag	IPv4 route map route-tag.	integer	Minimum value: 0 Maximum value: 4294967295
sla-compare-method	Method to compare SLA value for sla and load balance mode.	option	-
	Option	Description	
	<i>order</i>	Compare SLA value based on the order of health-check.	
	<i>number</i>	Compare SLA value based on the number of satisfied health-check. Limits health-checks to only configured member interfaces.	
src <name>	Source address name. Address or address group name.	string	Maximum length: 79
src-negate	Enable/disable negation of source address match.	option	-
	Option	Description	
	<i>enable</i>	Enable source address negation.	
	<i>disable</i>	Disable source address negation.	
src6 <name>	Source address6 name. Address6 or address6 group name.	string	Maximum length: 79
standalone-action	Enable/disable service when selected neighbor role is standalone while service role is not standalone.	option	-
	Option	Description	
	<i>enable</i>	Enable service when selected neighbor role is standalone.	
	<i>disable</i>	Disable service when selected neighbor role is standalone.	
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
status	Enable/disable SD-WAN service.	option	-
	Option	Description	
	<i>enable</i>	Enable virtual WAN link service.	
	<i>disable</i>	Disable virtual WAN link service.	
tos	Type of service bit pattern.	user	Not Specified
tos-mask	Type of service evaluated bits.	user	Not Specified
users <name>	User name.	string	Maximum
	User name.		length: 79

config sla

Parameter	Description	Type	Size
health-check	Virtual WAN Link health-check.	string	Maximum length: 35
id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295

config zone

Parameter	Description	Type	Size
name	Zone name.	string	Maximum length: 35

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 poweroff-bypass [enable|disable]
        set poweron-bypass [enable|disable]
        set vlan-filter {user}
        set wildcard-vlan [enable|disable]
    next
end
```

config system virtual-wire-pair

Parameter	Description	Type	Size
member <interface-name>	Interfaces belong to the virtual-wire-pair. Interface name.	string	Maximum length: 79
name	Virtual-wire-pair name. Must be a unique interface name.	string	Maximum length: 11
poweroff-bypass *	Enable/disable interface bypass state when power off.	option	-
		Option	Description
		<i>enable</i>	Enable bypass when power off.
		<i>disable</i>	Disable bypass when power off.
poweron-bypass *	Enable/disable interface bypass state when power on.	option	-
		Option	Description
		<i>enable</i>	Enable bypass when power on.
		<i>disable</i>	Disable bypass when power on.
vlan-filter	Set VLAN filters.	user	Not Specified
wildcard-vlan	Enable/disable wildcard VLAN.	option	-
		Option	Description
		<i>enable</i>	Enable wildcard VLAN.
		<i>disable</i>	Disable wildcard VLAN.

* This parameter may not exist in some models.

config system vxlan

Configure VXLAN devices.

```
config system vxlan
  Description: Configure VXLAN devices.
  edit <name>
    set dstport {integer}
    set interface {string}
    set ip-version [ipv4-unicast|ipv6-unicast|...]
    set multicast-ttl {integer}
    set remote-ip <ip1>, <ip2>, ...
```

```

        set remote-ip6 <ip61>, <ip62>, ...
        set vni {integer}
    next
end

```

config system vxlan

Parameter	Description	Type	Size										
dstport	VXLAN destination port (1 - 65535, default = 4789).	integer	Minimum value: 1 Maximum value: 65535										
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15										
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast or multicast.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-unicast</td><td>Use IPv4 unicast addressing over the VXLAN.</td></tr><tr><td>ipv6-unicast</td><td>Use IPv6 unicast addressing over the VXLAN.</td></tr><tr><td>ipv4-multicast</td><td>Use IPv4 multicast addressing over the VXLAN.</td></tr><tr><td>ipv6-multicast</td><td>Use IPv6 multicast addressing over the VXLAN.</td></tr></table>	Option	Description	ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.	ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.	ipv4-multicast	Use IPv4 multicast addressing over the VXLAN.	ipv6-multicast	Use IPv6 multicast addressing over the VXLAN.		
	Option	Description											
	ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.											
	ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.											
	ipv4-multicast	Use IPv4 multicast addressing over the VXLAN.											
ipv6-multicast	Use IPv6 multicast addressing over the VXLAN.												
multicast-ttl	VXLAN multicast TTL (1-255, default = 0).	integer	Minimum value: 1 Maximum value: 255										
name	VXLAN device or interface name. Must be a unique interface name.	string	Maximum length: 15										
remote-ip <ip>	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN. IPv4 address.	string	Maximum length: 15										
remote-ip6 <ip6>	IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN. IPv6 address.	string	Maximum length: 45										
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215										

config system wccp

Configure WCCP.

```
config system wccp
  Description: Configure WCCP.
  edit <service-id>
    set assignment-bucket-format [wccp-v2|cisco-implementation]
    set assignment-dstaddr-mask {ipv4-netmask-any}
    set assignment-method [HASH|MASK|...]
    set assignment-srcaddr-mask {ipv4-netmask-any}
    set assignment-weight {integer}
    set authentication [enable|disable]
    set cache-engine-method [GRE|L2]
    set cache-id {ipv4-address}
    set forward-method [GRE|L2|...]
    set group-address {ipv4-address-multicast}
    set password {password}
    set ports {user}
    set ports-defined [source|destination]
    set primary-hash {option1}, {option2}, ...
    set priority {integer}
    set protocol {integer}
    set return-method [GRE|L2|...]
    set router-id {ipv4-address}
    set router-list {user}
    set server-list {user}
    set server-type [forward|proxy]
    set service-type [auto|standard|...]
  next
end
```

config system wccp

Parameter	Description	Type	Size						
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wccp-v2</td><td>WCCP-v2 bucket format.</td></tr><tr><td>cisco-implementation</td><td>Cisco bucket format.</td></tr></table>	Option	Description	wccp-v2	WCCP-v2 bucket format.	cisco-implementation	Cisco bucket format.		
	Option	Description							
	wccp-v2	WCCP-v2 bucket format.							
cisco-implementation	Cisco bucket format.								
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified						
assignment-method	Hash key assignment preference.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>HASH</i>	HASH assignment method.	
	<i>MASK</i>	MASK assignment method.	
	<i>any</i>	HASH or MASK.	
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255
authentication	Enable/disable MD5 authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable MD5 authentication.	
	<i>disable</i>	Disable MD5 authentication.	
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-
	Option	Description	
	<i>GRE</i>	GRE encapsulation.	
	<i>L2</i>	L2 rewrite.	
cache-id	IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.	ipv4-address	Not Specified
forward-method	Method used to forward traffic to the cache servers.	option	-
	Option	Description	
	<i>GRE</i>	GRE encapsulation.	
	<i>L2</i>	L2 rewrite.	
	<i>any</i>	GRE or L2.	
group-address	IP multicast address used by the cache routers. For the FortiGate to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified
password	Password for MD5 authentication.	password	Not Specified

Parameter	Description	Type	Size
ports	Service ports.	user	Not Specified
ports-defined	Match method.	option	-
	Option	Description	
	source	Source port match.	
	destination	Destination port match.	
primary-hash	Hash method.	option	-
	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
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.	
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
router-list	IP addresses of one or more WCCP routers.	user	Not Specified
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified
server-type	Cache server type.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>forward</i>	Forward server.	
	<i>proxy</i>	Proxy server.	
service-id	Service ID.	string	Maximum length: 3
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-
	Option	Description	
	<i>auto</i>	auto	
	<i>standard</i>	Standard service.	
	<i>dynamic</i>	Dynamic service.	

config system wireless ap-status



This command is available for model(s): FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure accepted wireless AP.

```

config system wireless ap-status
    Description: Configure accepted wireless AP.
    edit <id>
        set bssid {mac-address}
        set ssid {string}
        set status [rogue|accepted|...]
    next
end

```

config system wireless ap-status

Parameter	Description	Type	Size
bssid	AP's BSSID.	mac-address	Not Specified
id	AP ID.	integer	Minimum value: 0 Maximum value: 4294967295
ssid	AP's ssid	string	Maximum length: 32
status	AP status.	option	-

Option	Description
<i>rogue</i>	Rogue.
<i>accepted</i>	Accepted.
<i>suppressed</i>	Suppressed.

config system wireless settings



This command is available for model(s): FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 51E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 100D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 300E, FortiGate 301E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001D, FortiGate 5001E1, FortiGate 5001E, FortiGate 500D, FortiGate 500E, FortiGate 501E, FortiGate 50E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 80F 2R, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Wireless radio configuration.

```
config system wireless settings
    Description: Wireless radio configuration.
    set band [802.11a|802.11b|...]
    set beacon-interval {integer}
    set bgscan [disable|enable]
    set bgscan-idle {integer}
    set bgscan-interval {integer}
    set channel {integer}
    set channel-bonding [enable|disable]
    set geography [World|Americas|...]
    set mode [CLIENT|AP|...]
    set power-level {integer}
    set rogue-scan [enable|disable]
    set rogue-scan-mac-adjacency {integer}
    set short-guard-interval [enable|disable]
end
```

config system wireless settings

Parameter	Description	Type	Size																										
band	Band.	option	-																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g.</td></tr><tr><td>802.11g-only</td><td>802.11g only.</td></tr><tr><td>802.11n</td><td>802.11n at 2.4G band.</td></tr><tr><td>802.11ng-only</td><td>802.11ng only at 2.4G band.</td></tr><tr><td>802.11n-only</td><td>802.11n only at 2.4G band.</td></tr><tr><td>802.11n-5G</td><td>802.11n at 5G band.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n only at 5G band.</td></tr><tr><td>802.11ac</td><td>802.11ac at 5G band.</td></tr><tr><td>802.11acn-only</td><td>802.11acn only at 5G band.</td></tr><tr><td>802.11ac-only</td><td>802.11ac only at 5G band.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g.	802.11g-only	802.11g only.	802.11n	802.11n at 2.4G band.	802.11ng-only	802.11ng only at 2.4G band.	802.11n-only	802.11n only at 2.4G band.	802.11n-5G	802.11n at 5G band.	802.11n-5G-only	802.11n only at 5G band.	802.11ac	802.11ac at 5G band.	802.11acn-only	802.11acn only at 5G band.	802.11ac-only	802.11ac only at 5G band.		
	Option	Description																											
	802.11a	802.11a.																											
	802.11b	802.11b.																											
	802.11g	802.11g.																											
	802.11g-only	802.11g only.																											
	802.11n	802.11n at 2.4G band.																											
	802.11ng-only	802.11ng only at 2.4G band.																											
	802.11n-only	802.11n only at 2.4G band.																											
	802.11n-5G	802.11n at 5G band.																											
	802.11n-5G-only	802.11n only at 5G band.																											
	802.11ac	802.11ac at 5G band.																											
	802.11acn-only	802.11acn only at 5G band.																											
	802.11ac-only	802.11ac only at 5G band.																											
beacon-interval	Beacon level (25 - 1000).	integer	Minimum value: 25 Maximum value: 1000																										
bgscan	Enable/disable background rogue AP scan.	option	-																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable background rogue AP scan.</td></tr><tr><td>enable</td><td>Enable background rogue AP scan.</td></tr></table>	Option	Description	disable	Disable background rogue AP scan.	enable	Enable background rogue AP scan.																						
	Option	Description																											
	disable	Disable background rogue AP scan.																											
enable	Enable background rogue AP scan.																												
bgscan-idle	Interval between scanning channels (100 - 1000 ms).	integer	Minimum value: 100 Maximum value: 1000																										
bgscan-interval	Interval between two rounds of scanning (15 - 3600 sec).	integer	Minimum value: 15 Maximum value: 3600																										

Parameter	Description	Type	Size
channel	Channel.	integer	Minimum value: 0 Maximum value: 4294967295
channel-bonding	Supported channel width.	option	-

Option	Description
<i>enable</i>	20/40 MHz.
<i>disable</i>	20 MHz.

geography	Geography.	option	-

Option	Description
<i>World</i>	World.
<i>Americas</i>	Americas.
<i>EMEA</i>	EMEA.
<i>Israel</i>	Israel.
<i>Japan</i>	Japan.

mode	Mode.	option	-

Option	Description
<i>CLIENT</i>	Client.
<i>AP</i>	Access point.
<i>SCAN</i>	Scan.

power-level	Power level (0 - 17).	integer	Minimum value: 0 Maximum value: 17

rogue-scan	Enable/disable rogue scan.	option	-

Option	Description
<i>enable</i>	Enable rogue scan.
<i>disable</i>	Disable rogue scan.

Parameter	Description	Type	Size
rogue-scan-mac-adjacency	MAC adjacency (0-31).	integer	Minimum value: 0 Maximum value: 31
short-guard-interval	Enable/disable short guard interval.	option	-

Option	Description
<i>enable</i>	400 ns long guard interval.
<i>disable</i>	800 ns short guard interval.

config system zone

Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.

```
config system zone
    Description: Configure zones to group two or more interfaces. When a zone is created you
    can configure policies for the zone instead of individual interfaces in the zone.
    edit <name>
        set description {string}
        set interface <interface-name1>, <interface-name2>, ...
        set intrazone [allow|deny]
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
    next
end
```

config system zone

Parameter	Description	Type	Size
description	Description.	string	Maximum length: 127
interface <interface-name>	Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined. Select interfaces to add to the zone.	string	Maximum length: 79

Parameter	Description	Type	Size
intrazone	Allow or deny traffic routing between different interfaces in the same zone (default = deny).	option	-
	Option	Description	
	<i>allow</i>	Allow traffic between interfaces in the zone.	
	<i>deny</i>	Deny traffic between interfaces in the zone.	
name	Zone name.	string	Maximum length: 35

config tagging

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

user

This section includes syntax for the following commands:

- [config user adgrp on page 1266](#)
- [config user domain-controller on page 1267](#)
- [config user exchange on page 1268](#)
- [config user fortitoken on page 1270](#)
- [config user fsso-polling on page 1275](#)
- [config user fsso on page 1271](#)
- [config user group on page 1277](#)
- [config user krb-keytab on page 1282](#)
- [config user ldap on page 1283](#)
- [config user local on page 1287](#)
- [config user password-policy on page 1291](#)
- [config user peer on page 1291](#)
- [config user peergrp on page 1293](#)
- [config user pop3 on page 1294](#)
- [config user quarantine on page 1295](#)
- [config user radius on page 1296](#)
- [config user saml on page 1306](#)
- [config user security-exempt-list on page 1307](#)
- [config user setting on page 1308](#)
- [config user tacacs+ on page 1312](#)

config user adgrp

Configure FSSO groups.

```
config user adgrp
    Description: Configure FSSO groups.
    edit <name>
        set id {integer}
        set server-name {string}
    next
end
```

config user adgrp

Parameter	Description	Type	Size
id	Group ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
name	Name.	string	Maximum length: 511
server-name	FSSO agent name.	string	Maximum length: 35

config user domain-controller

Configure domain controller entries.

```
config user domain-controller
  Description: Configure domain controller entries.
  edit <name>
    set domain-name {string}
    config extra-server
      Description: extra servers.
      edit <id>
        set ip-address {ipv4-address}
        set port {integer}
      next
    end
    set ip-address {ipv4-address}
    set ldap-server {string}
    set port {integer}
  next
end
```

config user domain-controller

Parameter	Description	Type	Size
domain-name	Domain DNS name.	string	Maximum length: 255
ip-address	Domain controller IP address.	ipv4-address	Not Specified
ldap-server	LDAP server name.	string	Maximum length: 35

Parameter	Description	Type	Size
name	Domain controller entry name.	string	Maximum length: 35
port	Port to be used for communication with the domain controller (default = 445).	integer	Minimum value: 0 Maximum value: 65535

config extra-server

Parameter	Description	Type	Size
id	Server ID.	integer	Minimum value: 1 Maximum value: 100
ip-address	Domain controller IP address.	ipv4-address	Not Specified
port	Port to be used for communication with the domain controller (default = 445).	integer	Minimum value: 0 Maximum value: 65535

config user exchange

Configure MS Exchange server entries.

```
config user exchange
    Description: Configure MS Exchange server entries.
    edit <name>
        set auth-level [connect|call|...]
        set auth-type [spnego|ntlm|...]
        set connect-protocol [rpc-over-tcp|rpc-over-http|...]
        set domain-name {string}
        set http-auth-type [basic|ntlm]
        set ip {ipv4-address-any}
        set kdc-ip <ipv41>, <ipv42>, ...
        set password {password}
        set server-name {string}
        set ssl-min-proto-version [default|SSLv3|...]
        set username {string}
    next
end
```

config user exchange

Parameter	Description	Type	Size												
auth-level	Authentication security level used for the RPC protocol layer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>connect</i></td><td>RPC authentication level 'connect'.</td></tr><tr><td><i>call</i></td><td>RPC authentication level 'call'.</td></tr><tr><td><i>packet</i></td><td>RPC authentication level 'packet'.</td></tr><tr><td><i>integrity</i></td><td>RPC authentication level 'integrity'.</td></tr><tr><td><i>privacy</i></td><td>RPC authentication level 'privacy'.</td></tr></table>	Option	Description	<i>connect</i>	RPC authentication level 'connect'.	<i>call</i>	RPC authentication level 'call'.	<i>packet</i>	RPC authentication level 'packet'.	<i>integrity</i>	RPC authentication level 'integrity'.	<i>privacy</i>	RPC authentication level 'privacy'.		
Option	Description														
<i>connect</i>	RPC authentication level 'connect'.														
<i>call</i>	RPC authentication level 'call'.														
<i>packet</i>	RPC authentication level 'packet'.														
<i>integrity</i>	RPC authentication level 'integrity'.														
<i>privacy</i>	RPC authentication level 'privacy'.														
auth-type	Authentication security type used for the RPC protocol layer.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spnego</i></td><td>Negotiate authentication.</td></tr><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>kerberos</i></td><td>Kerberos authentication.</td></tr></table>	Option	Description	<i>spnego</i>	Negotiate authentication.	<i>ntlm</i>	NTLM authentication.	<i>kerberos</i>	Kerberos authentication.						
Option	Description														
<i>spnego</i>	Negotiate authentication.														
<i>ntlm</i>	NTLM authentication.														
<i>kerberos</i>	Kerberos authentication.														
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rpc-over-tcp</i></td><td>Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.</td></tr><tr><td><i>rpc-over-http</i></td><td>Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td></tr><tr><td><i>rpc-over-https</i></td><td>Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td></tr></table>	Option	Description	<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.	<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.	<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.						
Option	Description														
<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.														
<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.														
<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.														
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79												
http-auth-type	Authentication security type used for the HTTP transport.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>ntlm</i></td><td>NTLM HTTP authentication.</td></tr></table>	Option	Description	<i>basic</i>	Basic HTTP authentication.	<i>ntlm</i>	NTLM HTTP authentication.								
Option	Description														
<i>basic</i>	Basic HTTP authentication.														
<i>ntlm</i>	NTLM HTTP authentication.														

Parameter	Description	Type	Size												
ip	Server IPv4 address.	ipv4-address-any	Not Specified												
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79												
name	MS Exchange server entry name.	string	Maximum length: 35												
password	Password for the specified username.	password	Not Specified												
server-name	MS Exchange server hostname.	string	Maximum length: 63												
ssl-min-protocol-version	Minimum SSL/TLS protocol version for HTTPS transport (default is to follow system global setting).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>			Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.
Option	Description														
default	Follow system global setting.														
SSLv3	SSLv3.														
TLSv1	TLSv1.														
TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.														
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64												

config user fortitoken

Configure FortiToken.

```

config user fortitoken
    Description: Configure FortiToken.
    edit <serial-number>
        set activation-code {string}
        set activation-expire {integer}
        set comments {var-string}
        set license {string}
        set os-ver {string}
        set reg-id {string}
        set seed {string}
        set status [active|lock]
    next
end

```

config user fortitoken

Parameter	Description	Type	Size
activation-code	Mobile token user activation-code.	string	Maximum length: 32
activation-expire	Mobile token user activation-code expire time.	integer	Minimum value: 0 Maximum value: 4294967295
comments	Comment.	var-string	Maximum length: 255
license	Mobile token license.	string	Maximum length: 31
os-ver	Device Mobile Version.	string	Maximum length: 15
reg-id	Device Reg ID.	string	Maximum length: 256
seed *	Token seed.	string	Maximum length: 200
serial-number	Serial number.	string	Maximum length: 16
status	Status	option	-

Option	Description
<i>active</i>	Activate FortiToken.
<i>lock</i>	Lock FortiToken.

* This parameter may not exist in some models.

config user fsso

Configure Fortinet Single Sign On (FSSO) agents.

```
config user fsso
  Description: Configure Fortinet Single Sign On (FSSO) agents.
  edit <name>
    set group-poll-interval {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ldap-poll [enable|disable]
    set ldap-poll-filter {string}
    set ldap-poll-interval {integer}
```

```

set ldap-server {string}
set password {password}
set password2 {password}
set password3 {password}
set password4 {password}
set password5 {password}
set port {integer}
set port2 {integer}
set port3 {integer}
set port4 {integer}
set port5 {integer}
set server {string}
set server2 {string}
set server3 {string}
set server4 {string}
set server5 {string}
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set ssl [enable|disable]
set ssl-trusted-cert {string}
set type [default|fortiems|...]
set user-info-server {string}
next
end

```

config user fsso

Parameter	Description	Type	Size
group-poll-interval	Interval in minutes within to fetch groups from FSSO server, or unset to disable.	integer	Minimum value: 1 Maximum value: 2880
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
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.	
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-

Parameter	Description	Type	Size

	Option	Description	
	<i>enable</i>	Enable automatic fetching of groups from LDAP server.	
	<i>disable</i>	Disable automatic fetching of groups from LDAP server.	

ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880
ldap-server	LDAP server to get group information.	string	Maximum length: 35
name	Name.	string	Maximum length: 35
password	Password of the first FSSO collector agent.	password	Not Specified
password2	Password of the second FSSO collector agent.	password	Not Specified
password3	Password of the third FSSO collector agent.	password	Not Specified
password4	Password of the fourth FSSO collector agent.	password	Not Specified
password5	Password of the fifth FSSO collector agent.	password	Not Specified
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535

Parameter	Description	Type	Size
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63
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
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
type	Server type.	option	-

Option	Description
<i>default</i>	All other unspecified types of servers.
<i>fortiems</i>	FortiClient EMS server.
<i>fortinac</i>	FortiNAC server.

Parameter	Description	Type	Size
	Option	Description	
	<i>fortiems-cloud</i>	FortiClient EMS Cloud server.	
user-info-server	LDAP server to get user information.	string	Maximum length: 35

config user fsso-polling

Configure FSSO active directory servers for polling mode.

```
config user fsso-polling
  Description: Configure FSSO active directory servers for polling mode.
  edit <id>
    config adgrp
      Description: LDAP Group Info.
      edit <name>
        next
      end
      set default-domain {string}
      set ldap-server {string}
      set logon-history {integer}
      set password {password}
      set polling-frequency {integer}
      set port {integer}
      set server {string}
      set smb-ntlmv1-auth [enable|disable]
      set smbv1 [enable|disable]
      set status [enable|disable]
      set user {string}
    next
  end
```

config user fsso-polling

Parameter	Description	Type	Size
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35
id	Active Directory server ID.	integer	Minimum value: 0 Maximum value: 4294967295
ldap-server	LDAP server name used in LDAP connection strings.	string	Maximum length: 35

Parameter	Description	Type	Size
logon-history	Number of hours of logon history to keep, 0 means keep all history.	integer	Minimum value: 0 Maximum value: 48
password	Password required to log into this Active Directory server	password	Not Specified
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63
smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-

Option	Description
<i>enable</i>	Enable support of NTLMv1 for Samba authentication.
<i>disable</i>	Disable support of NTLMv1 for Samba authentication.

smbv1	Enable/disable support of SMBv1 for Samba.	option	-

Option	Description
<i>enable</i>	Enable support of SMBv1 for Samba.
<i>disable</i>	Disable support of SMBv1 for Samba.

status	Enable/disable polling for the status of this Active Directory server.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

user	User name required to log into this Active Directory server.	string	Maximum length: 35

config adgrp

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 511

config user group

Configure user groups.

```
config user group
  Description: Configure user groups.
  edit <name>
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set authtimeout {integer}
    set company [optional|mandatory|...]
    set email [disable|enable]
    set expire {integer}
    set expire-type [immediately|first-successful-login]
    set group-type [firewall|fsso-service|...]
    config guest
      Description: Guest User.
      edit <id>
        set comment {var-string}
        set company {string}
        set email {string}
        set expiration {user}
        set mobile-phone {string}
        set name {string}
        set password {password}
        set sponsor {string}
        set user-id {string}
      next
    end
    set http-digest-realm {string}
    set id {integer}
  config match
    Description: Group matches.
    edit <id>
      set group-name {string}
      set server-name {string}
    next
  end
  set max-accounts {integer}
  set member <name1>, <name2>, ...
  set mobile-phone [disable|enable]
  set multiple-guest-add [disable|enable]
  set password [auto-generate|specify|...]
  set sms-custom-server {string}
  set sms-server [fortiguard|custom]
  set sponsor [optional|mandatory|...]
```

```

set sso-attribute-value {string}
set user-id [email|auto-generate|...]
set user-name [disable|enable]
next
end

```

config user group

Parameter	Description	Type	Size
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 (0 - 100).	integer	Minimum value: 0 Maximum value: 100
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 Maximum value: 43200
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.	
expire	Time in seconds before guest user accounts expire. (1 - 31536000 sec)	integer	Minimum value: 1 Maximum value: 31536000
expire-type	Determine when the expiration countdown begins.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediately</i></td><td>Immediately.</td></tr><tr><td><i>first-successful-login</i></td><td>First successful login.</td></tr></table>	Option	Description	<i>immediately</i>	Immediately.	<i>first-successful-login</i>	First successful login.						
	Option	Description											
	<i>immediately</i>	Immediately.											
<i>first-successful-login</i>	First successful login.												
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>firewall</i></td><td>Firewall.</td></tr><tr><td><i>fsso-service</i></td><td>Fortinet Single Sign-On Service.</td></tr><tr><td><i>rsso</i></td><td>RADIUS based Single Sign-On Service.</td></tr><tr><td><i>guest</i></td><td>Guest.</td></tr></table>	Option	Description	<i>firewall</i>	Firewall.	<i>fsso-service</i>	Fortinet Single Sign-On Service.	<i>rsso</i>	RADIUS based Single Sign-On Service.	<i>guest</i>	Guest.		
	Option	Description											
	<i>firewall</i>	Firewall.											
	<i>fsso-service</i>	Fortinet Single Sign-On Service.											
	<i>rsso</i>	RADIUS based Single Sign-On Service.											
<i>guest</i>	Guest.												
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35										
id	Group ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295										
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 1024 **										
member <name>	Names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Group member name.	string	Maximum length: 511										
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Enable setting.</td></tr><tr><td><i>enable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.						
	Option	Description											
	<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.												
multiple-guest-add	Enable/disable addition of multiple guests.	option	-										

Parameter	Description	Type	Size
	Option Description		
	<i>disable</i>	Enable setting.	
	<i>enable</i>	Disable setting.	
name	Group name.	string	Maximum length: 35
password	Guest user password type.	option	-
	Option Description		
	<i>auto-generate</i>	Automatically generate.	
	<i>specify</i>	Specify.	
	<i>disable</i>	Disable.	
sms-custom-server	SMS server.	string	Maximum length: 35
sms-server	Send SMS through FortiGuard or other external server.	option	-
	Option Description		
	<i>fortiguard</i>	Send SMS by FortiGuard.	
	<i>custom</i>	Send SMS by custom server.	
sponsor	Set the action for the sponsor guest user field.	option	-
	Option Description		
	<i>optional</i>	Optional.	
	<i>mandatory</i>	Mandatory.	
	<i>disabled</i>	Disabled.	
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511
user-id	Guest user ID type.	option	-
	Option Description		
	<i>email</i>	Email address.	
	<i>auto-generate</i>	Automatically generate.	
	<i>specify</i>	Specify.	

Parameter	Description	Type	Size
user-name	Enable/disable the guest user name entry.	option	-

Option	Description
<i>disable</i>	Enable setting.
<i>enable</i>	Disable setting.

** Values may differ between models.

config guest

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
company	Set the action for the company guest user field.	string	Maximum length: 35
email	Email.	string	Maximum length: 64
expiration	Expire time.	user	Not Specified
id	Guest ID.	integer	Minimum value: 0 Maximum value: 4294967295
mobile-phone	Mobile phone.	string	Maximum length: 35
name	Guest name.	string	Maximum length: 64
password	Guest password.	password	Not Specified
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35
user-id	Guest ID.	string	Maximum length: 64

config match

Parameter	Description	Type	Size
group-name	Name of matching user or group on remote authentication server.	string	Maximum length: 511

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
server-name	Name of remote auth server.	string	Maximum length: 35

config user krb-keytab

Configure Kerberos keytab entries.

```
config user krb-keytab
    Description: Configure Kerberos keytab entries.
    edit <name>
        set keytab {string}
        set ldap-server {string}
        set pac-data [enable|disable]
        set principal {string}
    next
end
```

config user krb-keytab

Parameter	Description	Type	Size
keytab	base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191
ldap-server	LDAP server name.	string	Maximum length: 35
name	Kerberos keytab entry name.	string	Maximum length: 35
pac-data	Enable/disable parsing PAC data in the ticket.	option	-
	Option Description		
	<i>enable</i>	Enable parsing PAC data in the ticket.	
	<i>disable</i>	Disable parsing PAC data in the ticket.	
principal	Kerberos service principal, e.g. HTTP/fgt.example.com@EXAMPLE.COM.	string	Maximum length: 511

config user ldap

Configure LDAP server entries.

```
config user ldap
  Description: Configure LDAP server entries.
  edit <name>
    set account-key-filter {string}
    set account-key-processing [same|strip]
    set ca-cert {string}
    set cnid {string}
    set dn {string}
    set group-filter {string}
    set group-member-check [user-attr|group-object|...]
    set group-object-filter {string}
    set group-search-base {string}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set member-attr {string}
    set obtain-user-info [enable|disable]
    set password {password}
    set password-expiry-warning [enable|disable]
    set password-renewal [enable|disable]
    set port {integer}
    set search-type {option1}, {option2}, ...
    set secondary-server {string}
    set secure [disable|starttls|...]
    set server {string}
    set server-identity-check [enable|disable]
    set source-ip {ipv4-address}
    set ssl-min-proto-version [default|SSLv3|...]
    set tertiary-server {string}
    set two-factor [disable|fortitoken-cloud]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set type [simple|anonymous|...]
    set user-info-exchange-server {string}
    set username {string}
  next
end
```

config user ldap

Parameter	Description	Type	Size
account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>same</i></td><td>Same as UPN.</td></tr><tr><td><i>strip</i></td><td>Strip domain string from UPN.</td></tr></table>	Option	Description	<i>same</i>	Same as UPN.	<i>strip</i>	Strip domain string from UPN.				
	Option	Description									
	<i>same</i>	Same as UPN.									
<i>strip</i>	Strip domain string from UPN.										
ca-cert	CA certificate name.	string	Maximum length: 79								
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								
group-filter	Filter used for group matching.	string	Maximum length: 2047								
group-member-check	Group member checking methods.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user-attr</i></td><td>User attribute checking.</td></tr><tr><td><i>group-object</i></td><td>Group object checking.</td></tr><tr><td><i>posix-group-object</i></td><td>POSIX group object checking.</td></tr></table>	Option	Description	<i>user-attr</i>	User attribute checking.	<i>group-object</i>	Group object checking.	<i>posix-group-object</i>	POSIX group object checking.		
	Option	Description									
	<i>user-attr</i>	User attribute checking.									
	<i>group-object</i>	Group object checking.									
<i>posix-group-object</i>	POSIX group object checking.										
group-object-filter	Filter used for group searching.	string	Maximum length: 2047								
group-search-base	Search base used for group searching.	string	Maximum length: 511								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
	Option	Description									
	<i>auto</i>	Set outgoing interface automatically.									
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.										
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63								

Parameter	Description	Type	Size						
name	LDAP server entry name.	string	Maximum length: 35						
obtain-user-info	Enable/disable obtaining of user information.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable obtaining of user information.</td></tr><tr><td><i>disable</i></td><td>Disable obtaining of user information.</td></tr></table>	Option	Description	<i>enable</i>	Enable obtaining of user information.	<i>disable</i>	Disable obtaining of user information.		
Option	Description								
<i>enable</i>	Enable obtaining of user information.								
<i>disable</i>	Disable obtaining of user information.								
password	Password for initial binding.	password	Not Specified						
password-expiry-warning	Enable/disable password expiry warnings.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password expiry warnings.</td></tr><tr><td><i>disable</i></td><td>Disable password expiry warnings.</td></tr></table>	Option	Description	<i>enable</i>	Enable password expiry warnings.	<i>disable</i>	Disable password expiry warnings.		
Option	Description								
<i>enable</i>	Enable password expiry warnings.								
<i>disable</i>	Disable password expiry warnings.								
password-renewal	Enable/disable online password renewal.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable online password renewal.</td></tr><tr><td><i>disable</i></td><td>Disable online password renewal.</td></tr></table>	Option	Description	<i>enable</i>	Enable online password renewal.	<i>disable</i>	Disable online password renewal.		
Option	Description								
<i>enable</i>	Enable online password renewal.								
<i>disable</i>	Disable online password renewal.								
port	Port to be used for communication with the LDAP server (default = 389).	integer	Minimum value: 1 Maximum value: 65535						
search-type	Search type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>recursive</i></td><td>Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.</td></tr></table>	Option	Description	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.				
Option	Description								
<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.								
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63						
secure	Port to be used for authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>No SSL.</td></tr></table>	Option	Description	<i>disable</i>	No SSL.				
Option	Description								
<i>disable</i>	No SSL.								

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>starttls</i></td><td>Use StartTLS.</td></tr><tr><td><i>ldaps</i></td><td>Use LDAPS.</td></tr></table>	Option	Description	<i>starttls</i>	Use StartTLS.	<i>ldaps</i>	Use LDAPS.								
	Option	Description													
	<i>starttls</i>	Use StartTLS.													
<i>ldaps</i>	Use LDAPS.														
server	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	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server identity check.</td></tr><tr><td><i>disable</i></td><td>Disable server identity check.</td></tr></table>	Option	Description	<i>enable</i>	Enable server identity check.	<i>disable</i>	Disable server identity check.								
	Option	Description													
	<i>enable</i>	Enable server identity check.													
<i>disable</i>	Disable server identity check.														
source-ip	Source IP for communications to LDAP server.	ipv4-address	Not Specified												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.		
	Option	Description													
	<i>default</i>	Follow system global setting.													
	<i>SSLv3</i>	SSLv3.													
	<i>TLSv1</i>	TLSv1.													
	<i>TLSv1-1</i>	TLSv1.1.													
<i>TLSv1-2</i>	TLSv1.2.														
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63												
two-factor	Enable/disable two-factor authentication.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable two-factor authentication.</td></tr><tr><td><i>fortitoken-cloud</i></td><td>FortiToken Cloud Service.</td></tr></table>	Option	Description	<i>disable</i>	disable two-factor authentication.	<i>fortitoken-cloud</i>	FortiToken Cloud Service.								
	Option	Description													
	<i>disable</i>	disable two-factor authentication.													
<i>fortitoken-cloud</i>	FortiToken Cloud Service.														
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortitoken</i></td><td>FortiToken authentication.</td></tr></table>	Option	Description	<i>fortitoken</i>	FortiToken authentication.										
	Option	Description													
<i>fortitoken</i>	FortiToken authentication.														

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>email</td><td>Email one time password.</td></tr><tr><td>sms</td><td>SMS one time password.</td></tr></table>	Option	Description	email	Email one time password.	sms	SMS one time password.				
	Option	Description									
	email	Email one time password.									
sms	SMS one time password.										
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>email</td><td>Email notification for activation code.</td></tr><tr><td>sms</td><td>SMS notification for activation code.</td></tr></table>	Option	Description	email	Email notification for activation code.	sms	SMS notification for activation code.				
	Option	Description									
	email	Email notification for activation code.									
sms	SMS notification for activation code.										
type	Authentication type for LDAP searches.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>simple</td><td>Simple password authentication without search.</td></tr><tr><td>anonymous</td><td>Bind using anonymous user search.</td></tr><tr><td>regular</td><td>Bind using username/password and then search.</td></tr></table>	Option	Description	simple	Simple password authentication without search.	anonymous	Bind using anonymous user search.	regular	Bind using username/password and then search.		
	Option	Description									
	simple	Simple password authentication without search.									
	anonymous	Bind using anonymous user search.									
regular	Bind using username/password and then search.										
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35								
username	Username (full DN) for initial binding.	string	Maximum length: 511								

config user local

Configure local users.

```
config user local
    Description: Configure local users.
    edit <name>
        set auth-concurrent-override [enable|disable]
        set auth-concurrent-value {integer}
        set authtimeout {integer}
        set email-to {string}
        set fortitoken {string}
        set id {integer}
        set ldap-server {string}
        set passwd {password}
        set passwd-policy {string}
        set passwd-time {user}
        set ppk-identity {string}
        set ppk-secret {password-3}
        set radius-server {string}
```

```

    set sms-custom-server {string}
    set sms-phone {string}
    set sms-server [fortiguard|custom]
    set status [enable|disable]
    set tacacs+-server {string}
    set two-factor [disable|fortitoken|...]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set type [password|radius|...]
    set username-sensitivity [disable|enable]
    set workstation {string}
next
end

```

config user local

Parameter	Description	Type	Size
auth-concurrent-override	Enable/disable overriding the policy-auth-concurrent under config system global.	option	-
	Option	Description	
	<i>enable</i>	Enable auth-concurrent-override.	
	<i>disable</i>	Disable auth-concurrent-override.	
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440
email-to	Two-factor recipient's email address.	string	Maximum length: 63
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16
id	User ID. Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35

Parameter	Description	Type	Size						
name	User name.	string	Maximum length: 64						
passwd	User's password.	password	Not Specified						
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35						
passwd-time	Time of the last password update.	user	Not Specified						
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35						
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified						
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35						
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35						
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15						
sms-server	Send SMS through FortiGuard or other external server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>			Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.
Option	Description								
<i>fortiguard</i>	Send SMS by FortiGuard.								
<i>custom</i>	Send SMS by custom server.								
status	Enable/disable allowing the local user to authenticate with the FortiGate unit.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user.</td></tr><tr><td><i>disable</i></td><td>Disable user.</td></tr></table>			Option	Description	<i>enable</i>	Enable user.	<i>disable</i>	Disable user.
Option	Description								
<i>enable</i>	Enable user.								
<i>disable</i>	Disable user.								
tacacs+-server	Name of TACACS+ server with which the user must authenticate.	string	Maximum length: 35						
two-factor	Enable/disable two-factor authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable</td></tr><tr><td><i>fortitoken</i></td><td>FortiToken</td></tr></table>			Option	Description	<i>disable</i>	disable	<i>fortitoken</i>	FortiToken
Option	Description								
<i>disable</i>	disable								
<i>fortitoken</i>	FortiToken								

Parameter	Description	Type	Size
	Option	Description	
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.	
	<i>email</i>	Email authentication code.	
	<i>sms</i>	SMS authentication code.	
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-
	Option	Description	
	<i>fortitoken</i>	FortiToken authentication.	
	<i>email</i>	Email one time password.	
	<i>sms</i>	SMS one time password.	
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-
	Option	Description	
	<i>email</i>	Email notification for activation code.	
	<i>sms</i>	SMS notification for activation code.	
type	Authentication method.	option	-
	Option	Description	
	<i>password</i>	Password authentication.	
	<i>radius</i>	RADIUS server authentication.	
	<i>tacacs+</i>	TACACS+ server authentication.	
	<i>ldap</i>	LDAP server authentication.	
username-sensitivity	Enable/disable case and accent sensitivity when performing username matching (accents are stripped and case is ignored when disabled).	option	-
	Option	Description	
	<i>disable</i>	Ignore case and accents. Username at prompt not required to match case or accents.	
	<i>enable</i>	Do not ignore case and accents. Username at prompt must be an exact match.	
workstation	Name of the remote user workstation, if you want to limit the user to authenticate only from a particular workstation.	string	Maximum length: 35

config user password-policy

Configure user password policy.

```
config user password-policy
  Description: Configure user password policy.
  edit <name>
    set expire-days {integer}
    set expired-password-renewal [enable|disable]
    set warn-days {integer}
  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						
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable renewal of a password that already is expired.</td></tr><tr><td><i>disable</i></td><td>Disable renewal of a password that already is expired.</td></tr></table>			Option	Description	<i>enable</i>	Enable renewal of a password that already is expired.	<i>disable</i>	Disable renewal of a password that already is expired.
	Option	Description							
	<i>enable</i>	Enable renewal of a password that already is expired.							
<i>disable</i>	Disable renewal of a password that already is expired.								
name	Password policy name.	string	Maximum length: 35						
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						

config user peer

Configure peer users.

```
config user peer
  Description: Configure peer users.
  edit <name>
    set ca {string}
    set cn {string}
    set cn-type [string|email|...]
    set ldap-mode [password|principal-name]
```

```

        set ldap-password {password}
        set ldap-server {string}
        set ldap-username {string}
        set mandatory-ca-verify [enable|disable]
        set ocsp-override-server {string}
        set passwd {password}
        set subject {string}
        set two-factor [enable|disable]
    next
end

```

config user peer

Parameter	Description	Type	Size
ca	Name of the CA certificate.	string	Maximum length: 127
cn	Peer certificate common name.	string	Maximum length: 255
cn-type	Peer certificate common name type.	option	-
	Option	Description	
	<i>string</i>	Normal string.	
	<i>email</i>	Email address.	
	<i>FQDN</i>	Fully Qualified Domain Name.	
	<i>ipv4</i>	IPv4 address.	
	<i>ipv6</i>	IPv6 address.	
ldap-mode	Mode for LDAP peer authentication.	option	-
	Option	Description	
	<i>password</i>	Username/password.	
	<i>principal-name</i>	Principal name.	
ldap-password	Password for LDAP server bind.	password	Not Specified
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
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	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
name	Peer name.	string	Maximum length: 35
ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35
passwd	Peer's password used for two-factor authentication.	password	Not Specified
subject	Peer certificate name constraints.	string	Maximum length: 255
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable 2-factor authentication.	
	<i>disable</i>	Disable 2-factor authentication.	

config user peergrp

Configure peer groups.

```
config user peergrp
    Description: Configure peer groups.
    edit <name>
        set member <name1>, <name2>, ...
    next
end
```

config user peergrp

Parameter	Description	Type	Size
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35
name	Peer group name.	string	Maximum length: 35

config user pop3

POP3 server entry configuration.

```
config user pop3
  Description: POP3 server entry configuration.
  edit <name>
    set port {integer}
    set secure [none|starttls|...]
    set server {string}
    set ssl-min-proto-version [default|SSLv3|...]
  next
end
```

config user pop3

Parameter	Description	Type	Size
name	POP3 server entry name.	string	Maximum length: 35
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535
secure	SSL connection.	option	-

Option	Description
<i>none</i>	None.
<i>starttls</i>	Use StartTLS.
<i>pop3s</i>	Use POP3 over SSL.

server	{<name_str ip_str>} server domain name or IP.	string	Maximum length: 63
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-

Option	Description
<i>default</i>	Follow system global setting.
<i>SSLv3</i>	SSLv3.
<i>TLSv1</i>	TLSv1.
<i>TLSv1-1</i>	TLSv1.1.
<i>TLSv1-2</i>	TLSv1.2.

config user quarantine

Configure quarantine support.

```
config user quarantine
  Description: Configure quarantine support.
  set quarantine [enable|disable]
  config targets
    Description: Quarantine entry to hold multiple MACs.
    edit <entry>
      set description {string}
      config macs
        Description: Quarantine MACs.
        edit <mac>
          set description {string}
          set parent {string}
        next
      end
    next
  end
  set traffic-policy {string}
end
```

config user quarantine

Parameter	Description	Type	Size
quarantine	Enable/disable quarantine.	option	-
	Option	Description	
	<i>enable</i>	Enable quarantine.	
	<i>disable</i>	Disable quarantine.	
traffic-policy *	Traffic policy for quarantined MACs.	string	Maximum length: 63

* This parameter may not exist in some models.

config targets

Parameter	Description	Type	Size
description	Description for the quarantine entry.	string	Maximum length: 63
entry	Quarantine entry name.	string	Maximum length: 63

config macs

Parameter	Description	Type	Size
description	Description for the quarantine MAC.	string	Maximum length: 63
mac	Quarantine MAC.	mac-address	Not Specified
parent	Parent entry name. Read-only.	string	Maximum length: 63

config user radius

Configure RADIUS server entries.

```
config user radius
  Description: Configure RADIUS server entries.
  edit <name>
    config accounting-server
      Description: Additional accounting servers.
      edit <id>
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set port {integer}
        set secret {password}
        set server {string}
        set source-ip {string}
        set status [enable|disable]
      next
    end
    set acct-all-servers [enable|disable]
    set acct-interim-interval {integer}
    set all-usergroup [disable|enable]
    set auth-type [auto|ms_chap_v2|...]
    set class <name1>, <name2>, ...
    set h3c-compatibility [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set nas-ip {ipv4-address}
    set password-encoding [auto|ISO-8859-1]
    set password-renewal [enable|disable]
    set radius-coa [enable|disable]
    set radius-port {integer}
    set rso [enable|disable]
    set rso-context-timeout {integer}
    set rso-endpoint-attribute [User-Name|NAS-IP-Address|...]
    set rso-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
    set rso-ep-one-ip-only [enable|disable]
    set rso-flush-ip-session [enable|disable]
    set rso-log-flags {option1}, {option2}, ...
    set rso-log-period {integer}
    set rso-radius-response [enable|disable]
    set rso-radius-server-port {integer}
```



```

set rso-secret {password}
set rso-validate-request-secret [enable|disable]
set secondary-secret {password}
set secondary-server {string}
set secret {password}
set server {string}
set source-ip {string}
set sso-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute-key {string}
set sso-attribute-value-override [enable|disable]
set tertiary-secret {password}
set tertiary-server {string}
set timeout {integer}
set use-management-vdom [enable|disable]
set username-case-sensitive [enable|disable]

```

next

end

config user radius

Parameter	Description	Type	Size						
acct-all-servers	Enable/disable sending of accounting messages to all configured servers (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send accounting messages to all configured servers.</td></tr><tr><td><i>disable</i></td><td>Send accounting message only to servers that are confirmed to be reachable.</td></tr></table>	Option	Description	<i>enable</i>	Send accounting messages to all configured servers.	<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.		
Option	Description								
<i>enable</i>	Send accounting messages to all configured servers.								
<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.								
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 600 Maximum value: 86400						
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not automatically include this server in a user group.</td></tr><tr><td><i>enable</i></td><td>Include this RADIUS server in every user group.</td></tr></table>	Option	Description	<i>disable</i>	Do not automatically include this server in a user group.	<i>enable</i>	Include this RADIUS server in every user group.		
Option	Description								
<i>disable</i>	Do not automatically include this server in a user group.								
<i>enable</i>	Include this RADIUS server in every user group.								
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Use PAP, MSCHAP_v2, and CHAP (in that order).</td></tr><tr><td><i>ms_chap_v2</i></td><td>Microsoft Challenge Handshake Authentication Protocol version 2.</td></tr></table>	Option	Description	<i>auto</i>	Use PAP, MSCHAP_v2, and CHAP (in that order).	<i>ms_chap_v2</i>	Microsoft Challenge Handshake Authentication Protocol version 2.		
Option	Description								
<i>auto</i>	Use PAP, MSCHAP_v2, and CHAP (in that order).								
<i>ms_chap_v2</i>	Microsoft Challenge Handshake Authentication Protocol version 2.								

Parameter	Description	Type	Size
	Option	Description	
	<i>ms_chap</i>	Microsoft Challenge Handshake Authentication Protocol.	
	<i>chap</i>	Challenge Handshake Authentication Protocol.	
	<i>pap</i>	Password Authentication Protocol.	
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable H3C compatibility.	
	<i>disable</i>	Disable H3C compatibility.	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15
interface-select-method	Specify how to select outgoing interface to reach server.	option	-
	Option	Description	
	<i>auto</i>	Set outgoing interface automatically.	
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	
	<i>specify</i>	Set outgoing interface manually.	
name	RADIUS server entry name.	string	Maximum length: 35
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
password-encoding	Password encoding.	option	-
	Option	Description	
	<i>auto</i>	Use original password encoding.	
	<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.	
password-renewal	Enable/disable password renewal.	option	-

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password renewal.</td></tr><tr><td><i>disable</i></td><td>Disable password renewal.</td></tr></table>	Option	Description	<i>enable</i>	Enable password renewal.	<i>disable</i>	Disable password renewal.								
Option	Description														
<i>enable</i>	Enable password renewal.														
<i>disable</i>	Disable password renewal.														
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS CoA.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS CoA.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS CoA.	<i>disable</i>	Disable RADIUS CoA.								
Option	Description														
<i>enable</i>	Enable RADIUS CoA.														
<i>disable</i>	Disable RADIUS CoA.														
radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535												
rsso	Enable/disable RADIUS based single sign on feature.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS based single sign on feature.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS based single sign on feature.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS based single sign on feature.	<i>disable</i>	Disable RADIUS based single sign on feature.								
Option	Description														
<i>enable</i>	Enable RADIUS based single sign on feature.														
<i>disable</i>	Disable RADIUS based single sign on feature.														
rsso-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												
rsso-endpoint-attribute	RADIUS attributes used to extract the user endpoint identifier from the RADIUS Start record.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>User-Name</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Netmask</i></td><td>Use this attribute.</td></tr><tr><td><i>Filter-Id</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.		
Option	Description														
<i>User-Name</i>	Use this attribute.														
<i>NAS-IP-Address</i>	Use this attribute.														
<i>Framed-IP-Address</i>	Use this attribute.														
<i>Framed-IP-Netmask</i>	Use this attribute.														
<i>Filter-Id</i>	Use this attribute.														

Parameter	Description	Type	Size

Option	Description
<i>Login-IP-Host</i>	Use this attribute.
<i>Reply-Message</i>	Use this attribute.
<i>Callback-Number</i>	Use this attribute.
<i>Callback-Id</i>	Use this attribute.
<i>Framed-Route</i>	Use this attribute.
<i>Framed-IPX-Network</i>	Use this attribute.
<i>Class</i>	Use this attribute.
<i>Called-Station-Id</i>	Use this attribute.
<i>Calling-Station-Id</i>	Use this attribute.
<i>NAS-Identifier</i>	Use this attribute.
<i>Proxy-State</i>	Use this attribute.
<i>Login-LAT-Service</i>	Use this attribute.
<i>Login-LAT-Node</i>	Use this attribute.
<i>Login-LAT-Group</i>	Use this attribute.
<i>Framed-AppleTalk-Zone</i>	Use this attribute.
<i>Acct-Session-Id</i>	Use this attribute.
<i>Acct-Multi-Session-Id</i>	Use this attribute.

rsso-endpoint-block-attribute RADIUS attributes used to block a user. option -

Option	Description
<i>User-Name</i>	Use this attribute.
<i>NAS-IP-Address</i>	Use this attribute.
<i>Framed-IP-Address</i>	Use this attribute.

Parameter	Description	Type	Size																																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>Framed-IP-Netmask</i></td><td>Use this attribute.</td></tr><tr><td><i>Filter-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-IP-Host</i></td><td>Use this attribute.</td></tr><tr><td><i>Reply-Message</i></td><td>Use this attribute.</td></tr><tr><td><i>Callback-Number</i></td><td>Use this attribute.</td></tr><tr><td><i>Callback-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-Route</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IPX-Network</i></td><td>Use this attribute.</td></tr><tr><td><i>Class</i></td><td>Use this attribute.</td></tr><tr><td><i>Called-Station-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Calling-Station-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-Identifier</i></td><td>Use this attribute.</td></tr><tr><td><i>Proxy-State</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Service</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Node</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Group</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-AppleTalk-Zone</i></td><td>Use this attribute.</td></tr><tr><td><i>Acct-Session-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Acct-Multi-Session-Id</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.		
	Option	Description																																									
	<i>Framed-IP-Netmask</i>	Use this attribute.																																									
	<i>Filter-Id</i>	Use this attribute.																																									
	<i>Login-IP-Host</i>	Use this attribute.																																									
	<i>Reply-Message</i>	Use this attribute.																																									
	<i>Callback-Number</i>	Use this attribute.																																									
	<i>Callback-Id</i>	Use this attribute.																																									
	<i>Framed-Route</i>	Use this attribute.																																									
	<i>Framed-IPX-Network</i>	Use this attribute.																																									
	<i>Class</i>	Use this attribute.																																									
	<i>Called-Station-Id</i>	Use this attribute.																																									
	<i>Calling-Station-Id</i>	Use this attribute.																																									
	<i>NAS-Identifier</i>	Use this attribute.																																									
	<i>Proxy-State</i>	Use this attribute.																																									
	<i>Login-LAT-Service</i>	Use this attribute.																																									
	<i>Login-LAT-Node</i>	Use this attribute.																																									
	<i>Login-LAT-Group</i>	Use this attribute.																																									
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.																																									
	<i>Acct-Session-Id</i>	Use this attribute.																																									
<i>Acct-Multi-Session-Id</i>	Use this attribute.																																										
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	-																																								

Parameter	Description	Type	Size																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr><tr><td><i>disable</i></td><td>Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr></table>	Option	Description	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.	<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.												
	Option	Description																	
	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																	
<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																		
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable flush user IP sessions on RADIUS accounting stop.</td></tr><tr><td><i>disable</i></td><td>Disable flush user IP sessions on RADIUS accounting stop.</td></tr></table>	Option	Description	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.	<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.												
	Option	Description																	
	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.																	
<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.																		
rsso-log-flags	Events to log.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol-error</i></td><td>Enable this log type.</td></tr><tr><td><i>profile-missing</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-stop-missed</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-event</i></td><td>Enable this log type.</td></tr><tr><td><i>endpoint-block</i></td><td>Enable this log type.</td></tr><tr><td><i>radiusd-other</i></td><td>Enable this log type.</td></tr><tr><td><i>none</i></td><td>Disable all logging.</td></tr></table>	Option	Description	<i>protocol-error</i>	Enable this log type.	<i>profile-missing</i>	Enable this log type.	<i>accounting-stop-missed</i>	Enable this log type.	<i>accounting-event</i>	Enable this log type.	<i>endpoint-block</i>	Enable this log type.	<i>radiusd-other</i>	Enable this log type.	<i>none</i>	Disable all logging.		
	Option	Description																	
	<i>protocol-error</i>	Enable this log type.																	
	<i>profile-missing</i>	Enable this log type.																	
	<i>accounting-stop-missed</i>	Enable this log type.																	
	<i>accounting-event</i>	Enable this log type.																	
	<i>endpoint-block</i>	Enable this log type.																	
<i>radiusd-other</i>	Enable this log type.																		
<i>none</i>	Disable all logging.																		
rsso-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-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending RADIUS response packets.</td></tr><tr><td><i>disable</i></td><td>Disable sending RADIUS response packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending RADIUS response packets.	<i>disable</i>	Disable sending RADIUS response packets.												
	Option	Description																	
	<i>enable</i>	Enable sending RADIUS response packets.																	
<i>disable</i>	Disable sending RADIUS response packets.																		

Parameter	Description	Type	Size
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 0 Maximum value: 65535
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-

Option	Description
<i>enable</i>	Enable validating RADIUS request shared secret.
<i>disable</i>	Disable validating RADIUS request shared secret.

secondary-secret	Secret key to access the secondary server.	password	Not Specified
secondary-server	{<name_str ip_str>} secondary RADIUS CN domain name or IP.	string	Maximum length: 63
secret	Pre-shared secret key used to access the primary RADIUS server.	password	Not Specified
server	Primary RADIUS server CN domain name or IP address.	string	Maximum length: 63
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63
sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-

Option	Description
<i>User-Name</i>	Use this attribute.
<i>NAS-IP-Address</i>	Use this attribute.
<i>Framed-IP-Address</i>	Use this attribute.
<i>Framed-IP-Netmask</i>	Use this attribute.
<i>Filter-Id</i>	Use this attribute.
<i>Login-IP-Host</i>	Use this attribute.
<i>Reply-Message</i>	Use this attribute.

Parameter	Description	Type	Size

Option	Description
<i>Callback-Number</i>	Use this attribute.
<i>Callback-Id</i>	Use this attribute.
<i>Framed-Route</i>	Use this attribute.
<i>Framed-IPX-Network</i>	Use this attribute.
<i>Class</i>	Use this attribute.
<i>Called-Station-Id</i>	Use this attribute.
<i>Calling-Station-Id</i>	Use this attribute.
<i>NAS-Identifier</i>	Use this attribute.
<i>Proxy-State</i>	Use this attribute.
<i>Login-LAT-Service</i>	Use this attribute.
<i>Login-LAT-Node</i>	Use this attribute.
<i>Login-LAT-Group</i>	Use this attribute.
<i>Framed-AppleTalk-Zone</i>	Use this attribute.
<i>Acct-Session-Id</i>	Use this attribute.
<i>Acct-Multi-Session-Id</i>	Use this attribute.

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
<i>enable</i>	Enable override old attribute value with new value for the same endpoint.
<i>disable</i>	Disable override old attribute value with new value for the same endpoint.

tertiary-secret	Secret key to access the tertiary server.	password	Not Specified
tertiary-server	{<name_str ip_str>} tertiary RADIUS CN domain name or IP.	string	Maximum length: 63

Parameter	Description	Type	Size						
timeout	Time in seconds between re-sending authentication requests.	integer	Minimum value: 1 Maximum value: 300						
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send requests using the management VDOM.</td></tr><tr><td><i>disable</i></td><td>Send requests using the current VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Send requests using the management VDOM.	<i>disable</i>	Send requests using the current VDOM.		
Option	Description								
<i>enable</i>	Send requests using the management VDOM.								
<i>disable</i>	Send requests using the current VDOM.								
username-case-sensitive	Enable/disable case sensitive user names.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username case-sensitive.</td></tr><tr><td><i>disable</i></td><td>Disable username case-sensitive.</td></tr></table>	Option	Description	<i>enable</i>	Enable username case-sensitive.	<i>disable</i>	Disable username case-sensitive.		
Option	Description								
<i>enable</i>	Enable username case-sensitive.								
<i>disable</i>	Disable username case-sensitive.								

config accounting-server

Parameter	Description	Type	Size								
id	ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
Option	Description										
<i>auto</i>	Set outgoing interface automatically.										
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.										

Parameter	Description	Type	Size
port	RADIUS accounting port number.	integer	Minimum value: 0 Maximum value: 65535
secret	Secret key.	password	Not Specified
server	{<name_str ip_str>} Server CN domain name or IP.	string	Maximum length: 63
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63
status	Status.	option	-

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

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 group-name {string}
        set idp-cert {string}
        set idp-entity-id {string}
        set idp-single-logout-url {string}
        set idp-single-sign-on-url {string}
        set single-logout-url {string}
        set single-sign-on-url {string}
        set user-name {string}
    next
end
```

config user saml

Parameter	Description	Type	Size
cert	Certificate to sign SAML messages.	string	Maximum length: 35

Parameter	Description	Type	Size
entity-id	SP entity ID.	string	Maximum length: 255
group-name	Group name in assertion statement.	string	Maximum length: 35
idp-cert	IDP Certificate name.	string	Maximum length: 35
idp-entity-id	IDP entity ID.	string	Maximum length: 255
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255
name	SAML server entry name.	string	Maximum length: 35
single-logout-url	SP single logout URL.	string	Maximum length: 255
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255
user-name	User name in assertion statement.	string	Maximum length: 35

config user security-exempt-list

Configure security exemption list.

```

config user security-exempt-list
    Description: Configure security exemption list.
    edit <name>
        set description {string}
        config rule
            Description: Configure rules for exempting users from captive portal
            authentication.
            edit <id>
                set dstaddr <name1>, <name2>, ...
                set service <name1>, <name2>, ...
                set srcaddr <name1>, <name2>, ...
            next
        end
    next
end

```

config user security-exempt-list

Parameter	Description	Type	Size
description	Description.	string	Maximum length: 127
name	Name of the exempt list.	string	Maximum length: 35

config rule

Parameter	Description	Type	Size
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
service <name>	Destination services. Service name.	string	Maximum length: 79
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79

config user setting

Configure user authentication setting.

```
config user setting
    Description: Configure user authentication setting.
    set auth-blackout-time {integer}
    set auth-ca-cert {string}
    set auth-cert {string}
    set auth-http-basic [enable|disable]
    set auth-invalid-max {integer}
    set auth-lockout-duration {integer}
    set auth-lockout-threshold {integer}
    set auth-on-demand [always|implicitly]
    set auth-portal-timeout {integer}
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
        TELNET.
        edit <id>
            set port {integer}
            set type [http|https|...]
        next
```

```

end
set auth-secure-http [enable|disable]
set auth-src-mac [enable|disable]
set auth-ssl-allow-renegotiation [enable|disable]
set auth-ssl-min-protocol-version [default|SSLv3|...]
set auth-timeout {integer}
set auth-timeout-type [idle-timeout|hard-timeout|...]
set auth-type {option1}, {option2}, ...
set per-policy-disclaimer [enable|disable]
set radius-ses-timeout-act [hard-timeout|ignore-timeout]
end

```

config user setting

Parameter	Description	Type	Size						
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-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35						
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35						
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100						
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295						
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10						

Parameter	Description	Type	Size								
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>always</i></td><td>Always trigger firewall authentication on demand.</td></tr><tr><td><i>implicitly</i></td><td>Implicitly trigger firewall authentication on demand.</td></tr></table>	Option	Description	<i>always</i>	Always trigger firewall authentication on demand.	<i>implicitly</i>	Implicitly trigger firewall authentication on demand.				
Option	Description										
<i>always</i>	Always trigger firewall authentication on demand.										
<i>implicitly</i>	Implicitly trigger firewall authentication on demand.										
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate (1 - 30 min, default 3 min).	integer	Minimum value: 1 Maximum value: 30								
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
auth-src-mac	Enable/disable source MAC for user identity.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source MAC for user identity.</td></tr><tr><td><i>disable</i></td><td>Disable source MAC for user identity.</td></tr></table>	Option	Description	<i>enable</i>	Enable source MAC for user identity.	<i>disable</i>	Disable source MAC for user identity.				
Option	Description										
<i>enable</i>	Enable source MAC for user identity.										
<i>disable</i>	Disable source MAC for user identity.										
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow SSL re-negotiation.</td></tr><tr><td><i>disable</i></td><td>Forbid SSL re-negotiation.</td></tr></table>	Option	Description	<i>enable</i>	Allow SSL re-negotiation.	<i>disable</i>	Forbid SSL re-negotiation.				
Option	Description										
<i>enable</i>	Allow SSL re-negotiation.										
<i>disable</i>	Forbid SSL re-negotiation.										
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.		
Option	Description										
<i>default</i>	Follow system global setting.										
<i>SSLv3</i>	SSLv3.										
<i>TLSv1</i>	TLSv1.										

Parameter	Description	Type	Size
	Option	Description	
	<i>TLSv1-1</i>	TLSv1.1.	
	<i>TLSv1-2</i>	TLSv1.2.	
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	
	<i>idle-timeout</i>	Idle timeout.	
	<i>hard-timeout</i>	Hard timeout.	
	<i>new-session</i>	New session timeout.	
auth-type	Supported firewall policy authentication protocols/methods.	option	-
	Option	Description	
	<i>http</i>	Allow HTTP authentication.	
	<i>https</i>	Allow HTTPS authentication.	
	<i>ftp</i>	Allow FTP authentication.	
	<i>telnet</i>	Allow TELNET authentication.	
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-
	Option	Description	
	<i>enable</i>	Enable per policy disclaimer.	
	<i>disable</i>	Disable per policy disclaimer.	
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-
	Option	Description	
	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.	
	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.	

config auth-ports

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535
type	Service type.	option	-

Option	Description
<i>http</i>	HTTP service.
<i>https</i>	HTTPS service.
<i>ftp</i>	FTP service.
<i>telnet</i>	TELNET service.

config user tacacs+

Configure TACACS+ server entries.

```
config user tacacs+
  Description: Configure TACACS+ server entries.
  edit <name>
    set authen-type [mschap|chap|...]
    set authorization [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set key {password}
    set port {integer}
    set secondary-key {password}
    set secondary-server {string}
    set server {string}
    set source-ip {string}
    set tertiary-key {password}
    set tertiary-server {string}
  next
end
```


config user tacacs+

Parameter	Description	Type	Size												
authen-type	Allowed authentication protocols/methods.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mschap</i></td><td>MSCHAP.</td></tr><tr><td><i>chap</i></td><td>CHAP.</td></tr><tr><td><i>pap</i></td><td>PAP.</td></tr><tr><td><i>ascii</i></td><td>ASCII.</td></tr><tr><td><i>auto</i></td><td>Use PAP, MSCHAP, and CHAP (in that order).</td></tr></table>	Option	Description	<i>mschap</i>	MSCHAP.	<i>chap</i>	CHAP.	<i>pap</i>	PAP.	<i>ascii</i>	ASCII.	<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).		
Option	Description														
<i>mschap</i>	MSCHAP.														
<i>chap</i>	CHAP.														
<i>pap</i>	PAP.														
<i>ascii</i>	ASCII.														
<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).														
authorization	Enable/disable TACACS+ authorization.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ authorization.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ authorization.	<i>disable</i>	Disable TACACS+ authorization.								
Option	Description														
<i>enable</i>	Enable TACACS+ authorization.														
<i>disable</i>	Disable TACACS+ authorization.														
interface	Specify outgoing interface to reach server.	string	Maximum length: 15												
interface-select-method	Specify how to select outgoing interface to reach server.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.						
Option	Description														
<i>auto</i>	Set outgoing interface automatically.														
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.														
<i>specify</i>	Set outgoing interface manually.														
key	Key to access the primary server.	password	Not Specified												
name	TACACS+ server entry name.	string	Maximum length: 35												
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535												
secondary-key	Key to access the secondary server.	password	Not Specified												
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63												
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63												

Parameter	Description	Type	Size
source-ip	source IP for communications to TACACS+ server.	string	Maximum length: 63
tertiary-key	Key to access the tertiary server.	password	Not Specified
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63

voip

This section includes syntax for the following commands:

- [config voip profile on page 1315](#)

config voip profile

Configure VoIP profiles.

```
config voip profile
  Description: Configure VoIP profiles.
  edit <name>
    set comment {var-string}
    config sccp
      Description: SCCP.
      set block-mcast [disable|enable]
      set log-call-summary [disable|enable]
      set log-violations [disable|enable]
      set max-calls {integer}
      set status [disable|enable]
      set verify-header [disable|enable]
    end
    config sip
      Description: SIP.
      set ack-rate {integer}
      set block-ack [disable|enable]
      set block-bye [disable|enable]
      set block-cancel [disable|enable]
      set block-geo-red-options [disable|enable]
      set block-info [disable|enable]
      set block-invite [disable|enable]
      set block-long-lines [disable|enable]
      set block-message [disable|enable]
      set block-notify [disable|enable]
      set block-options [disable|enable]
      set block-prack [disable|enable]
      set block-publish [disable|enable]
      set block-refer [disable|enable]
      set block-register [disable|enable]
      set block-subscribe [disable|enable]
      set block-unknown [disable|enable]
      set block-update [disable|enable]
      set bye-rate {integer}
      set call-keepalive {integer}
      set cancel-rate {integer}
      set contact-fixup [disable|enable]
      set hnt-restrict-source-ip [disable|enable]
      set hosted-nat-traversal [disable|enable]
      set info-rate {integer}
```

```
set invite-rate {integer}
set ips-rtp [disable|enable]
set log-call-summary [disable|enable]
set log-violations [disable|enable]
set malformed-header-allow [discard|pass|...]
set malformed-header-call-id [discard|pass|...]
set malformed-header-contact [discard|pass|...]
set malformed-header-content-length [discard|pass|...]
set malformed-header-content-type [discard|pass|...]
set malformed-header-cseq [discard|pass|...]
set malformed-header-expires [discard|pass|...]
set malformed-header-from [discard|pass|...]
set malformed-header-max-forwards [discard|pass|...]
set malformed-header-p-asserted-identity [discard|pass|...]
set malformed-header-rack [discard|pass|...]
set malformed-header-record-route [discard|pass|...]
set malformed-header-route [discard|pass|...]
set malformed-header-rseq [discard|pass|...]
set malformed-header-sdp-a [discard|pass|...]
set malformed-header-sdp-b [discard|pass|...]
set malformed-header-sdp-c [discard|pass|...]
set malformed-header-sdp-i [discard|pass|...]
set malformed-header-sdp-k [discard|pass|...]
set malformed-header-sdp-m [discard|pass|...]
set malformed-header-sdp-o [discard|pass|...]
set malformed-header-sdp-r [discard|pass|...]
set malformed-header-sdp-s [discard|pass|...]
set malformed-header-sdp-t [discard|pass|...]
set malformed-header-sdp-v [discard|pass|...]
set malformed-header-sdp-z [discard|pass|...]
set malformed-header-to [discard|pass|...]
set malformed-header-via [discard|pass|...]
set malformed-request-line [discard|pass|...]
set max-body-length {integer}
set max-dialogs {integer}
set max-idle-dialogs {integer}
set max-line-length {integer}
set message-rate {integer}
set nat-port-range {user}
set nat-trace [disable|enable]
set no-sdp-fixup [disable|enable]
set notify-rate {integer}
set open-contact-pinhole [disable|enable]
set open-record-route-pinhole [disable|enable]
set open-register-pinhole [disable|enable]
set open-via-pinhole [disable|enable]
set options-rate {integer}
set prack-rate {integer}
set preserve-override [disable|enable]
set provisional-invite-expiry-time {integer}
set publish-rate {integer}
set refer-rate {integer}
set register-contact-trace [disable|enable]
set register-rate {integer}
set rfc2543-branch [disable|enable]
set rtp [disable|enable]
```

```

        set ssl-algorithm [high|medium|...]
        set ssl-auth-client {string}
        set ssl-auth-server {string}
        set ssl-client-certificate {string}
        set ssl-client-renegotiation [allow|deny|...]
        set ssl-max-version [ssl-3.0|tls-1.0|...]
        set ssl-min-version [ssl-3.0|tls-1.0|...]
        set ssl-mode [off|full]
        set ssl-pfs [require|deny|...]
        set ssl-send-empty-frags [enable|disable]
        set ssl-server-certificate {string}
        set status [disable|enable]
        set strict-register [disable|enable]
        set subscribe-rate {integer}
        set unknown-header [discard|pass|...]
        set update-rate {integer}
    end
next
end

```

config voip profile

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

config sccp

Parameter	Description	Type	Size						
block-mcast	Enable/disable block multicast RTP connections.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
log-call-summary	Enable/disable log summary of SCCP calls.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
log-violations	Enable/disable logging of SCCP violations.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
max-calls	Maximum calls per minute per SCCP client (max 65535).	integer	Minimum value: 0 Maximum value: 65535
status	Enable/disable SCCP.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
verify-header	Enable/disable verify SCCP header content.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	

config sip

Parameter	Description	Type	Size
ack-rate	ACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
block-ack	Enable/disable block ACK requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-bye	Enable/disable block BYE requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	

Parameter	Description	Type	Size						
block-cancel	Enable/disable block CANCEL requests.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
block-geo-red-options	Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
block-info	Enable/disable block INFO requests.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
block-invite	Enable/disable block INVITE requests.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
block-long-lines	Enable/disable block requests with headers exceeding max-line-length.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
block-message	Enable/disable block MESSAGE requests.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
block-notify	Enable/disable block NOTIFY requests.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-options	Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-prack	Enable/disable block prack requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-publish	Enable/disable block PUBLISH requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-refer	Enable/disable block REFER requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-register	Enable/disable block REGISTER requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-subscribe	Enable/disable block SUBSCRIBE requests.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-unknown	Block unrecognized SIP requests (enabled by default).	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
block-update	Enable/disable block UPDATE requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
bye-rate	BYE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
call-keepalive	Continue tracking calls with no RTP for this many minutes.	integer	Minimum value: 0 Maximum value: 10080
cancel-rate	CANCEL request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
contact-fixup	Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
hnt-restrict-source-ip	Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
hosted-nat-traversal	Hosted NAT Traversal (HNT).	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
info-rate	INFO request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
invite-rate	INVITE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
ips-rtp	Enable/disable allow IPS on RTP.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
log-call-summary	Enable/disable logging of SIP call summary.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
log-violations	Enable/disable logging of SIP violations.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	

Parameter	Description	Type	Size								
malformed-header-allow	Action for malformed Allow header.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.		
Option	Description										
<i>discard</i>	Discard malformed messages.										
<i>pass</i>	Bypass malformed messages.										
<i>respond</i>	Respond with error code.										
malformed-header-call-id	Action for malformed Call-ID header.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.		
Option	Description										
<i>discard</i>	Discard malformed messages.										
<i>pass</i>	Bypass malformed messages.										
<i>respond</i>	Respond with error code.										
malformed-header-contact	Action for malformed Contact header.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.		
Option	Description										
<i>discard</i>	Discard malformed messages.										
<i>pass</i>	Bypass malformed messages.										
<i>respond</i>	Respond with error code.										
malformed-header-content-length	Action for malformed Content-Length header.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.		
Option	Description										
<i>discard</i>	Discard malformed messages.										
<i>pass</i>	Bypass malformed messages.										
<i>respond</i>	Respond with error code.										
malformed-header-content-type	Action for malformed Content-Type header.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.				
Option	Description										
<i>discard</i>	Discard malformed messages.										
<i>pass</i>	Bypass malformed messages.										

Parameter	Description	Type	Size
	Option	Description	
	<i>respond</i>	Respond with error code.	
malformed-header-cseq	Action for malformed CSeq header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-expires	Action for malformed Expires header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-from	Action for malformed From header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-max-forwards	Action for malformed Max-Forwards header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-p-asserted-identity	Action for malformed P-Asserted-Identity header.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-rack	Action for malformed RACK header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-record-route	Action for malformed Record-Route header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-route	Action for malformed Route header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-rseq	Action for malformed RSeq header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-a	Action for malformed SDP a line.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-b	Action for malformed SDP b line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-c	Action for malformed SDP c line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-i	Action for malformed SDP i line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-k	Action for malformed SDP k line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-m	Action for malformed SDP m line.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-o	Action for malformed SDP o line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-r	Action for malformed SDP r line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-s	Action for malformed SDP s line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-t	Action for malformed SDP t line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-v	Action for malformed SDP v line.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-sdp-z	Action for malformed SDP z line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-to	Action for malformed To header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-header-via	Action for malformed VIA header.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	
malformed-request-line	Action for malformed request line.	option	-
	Option	Description	
	<i>discard</i>	Discard malformed messages.	
	<i>pass</i>	Bypass malformed messages.	
	<i>respond</i>	Respond with error code.	

Parameter	Description	Type	Size
max-body-length	Maximum SIP message body length (0 meaning no limit).	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-idle-dialogs	Maximum number established but idle dialogs to retain (per policy).	integer	Minimum value: 0 Maximum value: 4294967295
max-line-length	Maximum SIP header line length (78-4096).	integer	Minimum value: 78 Maximum value: 4096
message-rate	MESSAGE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
nat-port-range	RTP NAT port range.	user	Not Specified
nat-trace	Enable/disable preservation of original IP in SDP i line.	option	-

Option	Description

<i>disable</i>	Disable status.

<i>enable</i>	Enable status.

no-sdp-fixup	Enable/disable no SDP fix-up.	option	-

Option	Description

<i>disable</i>	Disable status.

<i>enable</i>	Enable status.

Parameter	Description	Type	Size						
notify-rate	NOTIFY request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295						
open-contact-pinhole	Enable/disable open pinhole for non-REGISTER Contact port.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
open-record-route-pinhole	Enable/disable open pinhole for Record-Route port.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
open-register-pinhole	Enable/disable open pinhole for REGISTER Contact port.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
open-via-pinhole	Enable/disable open pinhole for Via port.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.		
Option	Description								
<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.								
options-rate	OPTIONS request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295						

Parameter	Description	Type	Size
prack-rate	PRACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
preserve-override	Override i line to preserve original IPS (default: append).	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
provisional-invite-expiry-time	Expiry time for provisional INVITE (10 - 3600 sec).	integer	Minimum value: 10 Maximum value: 3600
publish-rate	PUBLISH 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
register-contact-trace	Enable/disable trace original IP/port within the contact header of REGISTER requests.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
register-rate	REGISTER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295
rfc2543-branch	Enable/disable support via branch compliant with RFC 2543.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
rtp	Enable/disable create pinholes for RTP traffic to traverse firewall.	option	-
	Option	Description	
	<i>disable</i>	Disable status.	
	<i>enable</i>	Enable status.	
ssl-algorithm *	Relative strength of encryption algorithms accepted in negotiation.	option	-
	Option	Description	
	<i>high</i>	High encryption. Allow only AES and ChaCha.	
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	
ssl-auth-client *	Require a client certificate and authenticate it with the peer/peergrp.	string	Maximum length: 35
ssl-auth-server *	Authenticate the server's certificate with the peer/peergrp.	string	Maximum length: 35
ssl-client-certificate *	Name of Certificate to offer to server if requested.	string	Maximum length: 35
ssl-client-renegotiation *	Allow/block client renegotiation by server.	option	-
	Option	Description	
	<i>allow</i>	Allow a SSL client to renegotiate.	
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	
	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.	
ssl-max-version *	Highest SSL/TLS version to negotiate.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>ssl-3.0</i>	SSL 3.0.	
	<i>tls-1.0</i>	TLS 1.0.	
	<i>tls-1.1</i>	TLS 1.1.	
	<i>tls-1.2</i>	TLS 1.2.	
	<i>tls-1.3</i>	TLS 1.3.	
ssl-min-version *	Lowest SSL/TLS version to negotiate.	option	-
	Option	Description	
	<i>ssl-3.0</i>	SSL 3.0.	
	<i>tls-1.0</i>	TLS 1.0.	
	<i>tls-1.1</i>	TLS 1.1.	
	<i>tls-1.2</i>	TLS 1.2.	
	<i>tls-1.3</i>	TLS 1.3.	
ssl-mode *	SSL/TLS mode for encryption & decryption of traffic.	option	-
	Option	Description	
	<i>off</i>	No SSL.	
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.	
ssl-pfs *	SSL Perfect Forward Secrecy.	option	-
	Option	Description	
	<i>require</i>	PFS mandatory.	
	<i>deny</i>	PFS rejected.	
	<i>allow</i>	PFS allowed.	
ssl-send-empty-frags *	Send empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).	option	-
	Option	Description	
	<i>enable</i>	Send empty fragments.	
	<i>disable</i>	Do not send empty fragments.	

Parameter	Description	Type	Size								
ssl-server-certificate *	Name of Certificate return to the client in every SSL connection.	string	Maximum length: 35								
status	Enable/disable SIP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.				
Option	Description										
<i>disable</i>	Disable status.										
<i>enable</i>	Enable status.										
strict-register	Enable/disable only allow the registrar to connect.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.				
Option	Description										
<i>disable</i>	Disable status.										
<i>enable</i>	Enable status.										
subscribe-rate	SUBSCRIBE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295								
unknown-header	Action for unknown SIP header.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.		
Option	Description										
<i>discard</i>	Discard malformed messages.										
<i>pass</i>	Bypass malformed messages.										
<i>respond</i>	Respond with error code.										
update-rate	UPDATE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295								

* This parameter may not exist in some models.

vpn

This section includes syntax for the following commands:

- [config vpn certificate ca on page 1335](#)
- [config vpn certificate crl on page 1337](#)
- [config vpn certificate local on page 1338](#)
- [config vpn certificate ocsf-server on page 1341](#)
- [config vpn certificate remote on page 1342](#)
- [config vpn certificate setting on page 1343](#)
- [config vpn ipsec concentrator on page 1347](#)
- [config vpn ipsec forticlient on page 1347](#)
- [config vpn ipsec manualkey-interface on page 1350](#)
- [config vpn ipsec manualkey on page 1348](#)
- [config vpn ipsec phase1-interface on page 1371](#)
- [config vpn ipsec phase1 on page 1352](#)
- [config vpn ipsec phase2-interface on page 1403](#)
- [config vpn ipsec phase2 on page 1395](#)
- [config vpn l2tp on page 1411](#)
- [config vpn ocvpn on page 1412](#)
- [config vpn pptp on page 1415](#)
- [config vpn ssl settings on page 1416](#)
- [config vpn ssl web host-check-software on page 1428](#)
- [config vpn ssl web portal on page 1429](#)
- [config vpn ssl web realm on page 1445](#)
- [config vpn ssl web user-bookmark on page 1445](#)
- [config vpn ssl web user-group-bookmark on page 1450](#)

config vpn certificate ca

CA certificate.

```
config vpn certificate ca
  Description: CA certificate.
  edit <name>
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set ca {user}
    set range [global|vdom]
    set scep-url {string}
    set source [factory|user|...]
    set source-ip {ipv4-address}
```

```

        set ssl-inspection-trusted [enable|disable]
    next
end

```

config vpn certificate ca

Parameter	Description	Type	Size								
auto-update-days	Number of days to wait before requesting an updated CA certificate (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295								
auto-update-days-warning	Number of days before an expiry-warning message is generated (0 - 4294967295, 0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295								
ca	CA certificate as a PEM file.	user	Not Specified								
name	Name.	string	Maximum length: 79								
range	Either global or VDOM IP address range for the CA certificate.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>			Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
Option	Description										
<i>global</i>	Global range.										
<i>vdom</i>	VDOM IP address range.										
scep-url	URL of the SCEP server.	string	Maximum length: 255								
source	CA certificate source type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>			Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
Option	Description										
<i>factory</i>	Factory installed certificate.										
<i>user</i>	User generated certificate.										
<i>bundle</i>	Bundle file certificate.										
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified								
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Trusted CA for SSL inspection.	
	<i>disable</i>	Untrusted CA for SSL inspection.	

config vpn certificate crl

Certificate Revocation List as a PEM file.

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

config vpn certificate crl

Parameter	Description	Type	Size
crl	Certificate Revocation List as a PEM file.	user	Not Specified
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255
ldap-password	LDAP server user password.	password	Not Specified
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35
ldap-username	LDAP server user name.	string	Maximum length: 63
name	Name.	string	Maximum length: 35

Parameter	Description	Type	Size
range	Either global or VDOM IP address range for the certificate.	option	-
	Option	Description	
	<i>global</i>	Global range.	
	<i>vdom</i>	VDOM IP address range.	
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255
source	Certificate source type.	option	-
	Option	Description	
	<i>factory</i>	Factory installed certificate.	
	<i>user</i>	User generated certificate.	
	<i>bundle</i>	Bundle file certificate.	
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified
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
update-vdom	VDOM for CRL update.	string	Maximum length: 31

config vpn certificate local

Local keys and certificates.

```

config vpn certificate local
    Description: Local keys and certificates.
    edit <name>
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set ca-identifier {string}
        set certificate {user}
        set cmp-path {string}
        set cmp-regeneration-method [keyupdate|renewal]
        set cmp-server {string}
        set cmp-server-cert {string}
        set comments {string}
    
```

```

set csr {user}
set enroll-protocol [none|scep|...]
set ike-localid {string}
set ike-localid-type [asn1dn|fqdn]
set name-encoding [printable|utf8]
set password {password}
set private-key {user}
set range [global|vdom]
set scep-password {password}
set scep-url {string}
set source [factory|user|...]
set source-ip {ipv4-address}
set state {user}
next
end

```

config vpn certificate local

Parameter	Description	Type	Size						
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						
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255						
certificate	PEM format certificate.	user	Not Specified						
cmp-path	Path location inside CMP server.	string	Maximum length: 255						
cmp-regeneration-method	CMP auto-regeneration method.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>keyupate</i></td><td>Key Update.</td></tr><tr><td><i>renewal</i></td><td>Renewal.</td></tr></table>			Option	Description	<i>keyupate</i>	Key Update.	<i>renewal</i>	Renewal.
	Option	Description							
	<i>keyupate</i>	Key Update.							
<i>renewal</i>	Renewal.								
cmp-server	'ADDRESS:PORT' for CMP server.	string	Maximum length: 63						

Parameter	Description	Type	Size
cmp-server-cert	CMP server certificate.	string	Maximum length: 79
comments	Comment.	string	Maximum length: 511
csr	Certificate Signing Request.	user	Not Specified
enroll-protocol	Certificate enrollment protocol.	option	-
	Option	Description	
	<i>none</i>	None (default).	
	<i>scep</i>	Simple Certificate Enrollment Protocol.	
	<i>cmpv2</i>	Certificate Management Protocol Version 2.	
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	
	<i>asn1dn</i>	ASN.1 distinguished name.	
	<i>fqdn</i>	Fully qualified domain name.	
name	Name.	string	Maximum length: 35
name-encoding	Name encoding method for auto-regeneration.	option	-
	Option	Description	
	<i>printable</i>	Printable encoding (default).	
	<i>utf8</i>	UTF-8 encoding.	
password	Password as a PEM file.	password	Not Specified
private-key	PEM format key, encrypted with a password.	user	Not Specified
range	Either a global or VDOM IP address range for the certificate.	option	-
	Option	Description	
	<i>global</i>	Global range.	
	<i>vdom</i>	VDOM IP address range.	
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified

Parameter	Description	Type	Size
scep-url	SCEP server URL.	string	Maximum length: 255
source	Certificate source type.	option	-
	Option	Description	
	factory	Factory installed certificate.	
	user	User generated certificate.	
	bundle	Bundle file certificate.	
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified
state	Certificate Signing Request State. Read-only.	user	Not Specified

config vpn certificate ocsf-server

OCSP server configuration.

```

config vpn certificate ocsf-server
  Description: OCSP server configuration.
  edit <name>
    set cert {string}
    set secondary-cert {string}
    set secondary-url {string}
    set source-ip {ipv4-address}
    set unavail-action [revoke|ignore]
    set url {string}
  next
end

```

config vpn certificate ocsf-server

Parameter	Description	Type	Size
cert	OCSP server certificate.	string	Maximum length: 127
name	OCSP server entry name.	string	Maximum length: 35
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127

Parameter	Description	Type	Size						
source-ip	Source IP address for communications to the OCSP server.	ipv4-address	Not Specified						
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>revoke</td><td>Revoke certificate if server is unavailable.</td></tr><tr><td>ignore</td><td>Ignore OCSP check if server is unavailable.</td></tr></table>			Option	Description	revoke	Revoke certificate if server is unavailable.	ignore	Ignore OCSP check if server is unavailable.
	Option	Description							
	revoke	Revoke certificate if server is unavailable.							
ignore	Ignore OCSP check if server is unavailable.								
url	OCSP server URL.	string	Maximum length: 127						

config vpn certificate remote

Remote certificate as a PEM file.

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

config vpn certificate remote

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 35
range	Either the global or VDOM IP address range for the remote certificate.	option	-
	Option	Description	
	global	Global range.	
	vdom	VDOM IP address range.	
remote	Remote certificate.	user	Not Specified
source	Remote certificate source type.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>factory</i>	Factory installed certificate.	
	<i>user</i>	User generated certificate.	
	<i>bundle</i>	Bundle file certificate.	

config vpn certificate setting

VPN certificate setting.

```

config vpn certificate setting
    Description: VPN certificate setting.
    set certname-dsa1024 {string}
    set certname-dsa2048 {string}
    set certname-ecdsa256 {string}
    set certname-ecdsa384 {string}
    set certname-ecdsa521 {string}
    set certname-ed25519 {string}
    set certname-ed448 {string}
    set certname-rsa1024 {string}
    set certname-rsa2048 {string}
    set certname-rsa4096 {string}
    set check-ca-cert [enable|disable]
    set check-ca-chain [enable|disable]
    set cmp-key-usage-checking [enable|disable]
    set cmp-save-extra-certs [enable|disable]
    set cn-match [substring|value]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ocsf-default-server {string}
    set ocsf-option [certificate|server]
    set ocsf-status [enable|disable]
    set ssl-min-protol-version [default|SSLv3|...]
    set ssl-ocsp-source-ip {ipv4-address}
    set strict-crl-check [enable|disable]
    set strict-ocsp-check [enable|disable]
    set subject-match [substring|value]
end

```

config vpn certificate setting

Parameter	Description	Type	Size
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35

Parameter	Description	Type	Size
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
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
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted (default = enable).	option	-

Option	Description

<i>enable</i>	Enable verification of the user certificate.
<i>disable</i>	Disable verification of the user certificate.

check-ca-chain	Enable/disable verification of the entire certificate chain and pass authentication only if the chain is complete and all of the CAs in the chain are trusted (default = disable).	option	-

Option	Description

<i>enable</i>	Enable verification of the entire certificate chain.
<i>disable</i>	Disable verification of the entire certificate chain.

cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode (default = enable).	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server certificate key usage checking in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable server certificate key usage checking in CMP mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable server certificate key usage checking in CMP mode.	<i>disable</i>	Disable server certificate key usage checking in CMP mode.				
	Option	Description									
	<i>enable</i>	Enable server certificate key usage checking in CMP mode.									
<i>disable</i>	Disable server certificate key usage checking in CMP mode.										
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable saving extra certificates in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable saving extra certificates in CMP mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable saving extra certificates in CMP mode.	<i>disable</i>	Disable saving extra certificates in CMP mode.				
	Option	Description									
	<i>enable</i>	Enable saving extra certificates in CMP mode.									
<i>disable</i>	Disable saving extra certificates in CMP mode.										
cn-match	When searching for a matching certificate, control how to find matches in the cn attribute of the certificate subject name.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>substring</i></td><td>Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.</td></tr><tr><td><i>value</i></td><td>Find a match if the cn attribute value string is an exact match with the name being searched for.</td></tr></table>	Option	Description	<i>substring</i>	Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.	<i>value</i>	Find a match if the cn attribute value string is an exact match with the name being searched for.				
	Option	Description									
	<i>substring</i>	Find a match if any string in a certificate subject name cn attribute name matches the name being searched for.									
<i>value</i>	Find a match if the cn attribute value string is an exact match with the name being searched for.										
interface	Specify outgoing interface to reach server.	string	Maximum length: 15								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
	Option	Description									
	<i>auto</i>	Set outgoing interface automatically.									
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.									
<i>specify</i>	Set outgoing interface manually.										
ocsp-default-server	Default OCSP server.	string	Maximum length: 35								
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>certificate</i></td><td>Use URL from certificate.</td></tr><tr><td><i>server</i></td><td>Use URL from configured OCSP server.</td></tr></table>	Option	Description	<i>certificate</i>	Use URL from certificate.	<i>server</i>	Use URL from configured OCSP server.				
	Option	Description									
	<i>certificate</i>	Use URL from certificate.									
<i>server</i>	Use URL from configured OCSP server.										

Parameter	Description	Type	Size												
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
Option	Description														
<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.														
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections (default is to follow system global setting).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.		
Option	Description														
<i>default</i>	Follow system global setting.														
<i>SSLv3</i>	SSLv3.														
<i>TLSv1</i>	TLSv1.														
<i>TLSv1-1</i>	TLSv1.1.														
<i>TLSv1-2</i>	TLSv1.2.														
ssl-ocsp-source-ip	Source IP address to use to communicate with the OCSP server.	ipv4-address	Not Specified												
strict-crl-check	Enable/disable strict mode CRL checking.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict mode CRL checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict mode CRL checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict mode CRL checking.	<i>disable</i>	Disable strict mode CRL checking.								
Option	Description														
<i>enable</i>	Enable strict mode CRL checking.														
<i>disable</i>	Disable strict mode CRL checking.														
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict mode OCSP checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict mode OCSP checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict mode OCSP checking.	<i>disable</i>	Disable strict mode OCSP checking.								
Option	Description														
<i>enable</i>	Enable strict mode OCSP checking.														
<i>disable</i>	Disable strict mode OCSP checking.														
subject-match	When searching for a matching certificate, control how to find matches in the certificate subject name.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>substring</i></td><td>Find a match if any string in the certificate subject name matches the name being searched for.</td></tr><tr><td><i>value</i></td><td>Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.</td></tr></table>	Option	Description	<i>substring</i>	Find a match if any string in the certificate subject name matches the name being searched for.	<i>value</i>	Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.								
Option	Description														
<i>substring</i>	Find a match if any string in the certificate subject name matches the name being searched for.														
<i>value</i>	Find a match if any attribute value string in a certificate subject name is an exact match with the name being searched for.														

config vpn ipsec concentrator

Concentrator configuration.

```
config vpn ipsec concentrator
  Description: Concentrator configuration.
  edit <name>
    set member <name1>, <name2>, ...
    set src-check [disable|enable]
  next
end
```

config vpn ipsec concentrator

Parameter	Description	Type	Size
member <name>	Names of up to 3 VPN tunnels to add to the concentrator. Member name.	string	Maximum length: 79
name	Concentrator name.	string	Maximum length: 35
src-check	Enable to check source address of phase 2 selector. Disable to check only the destination selector.	option	-

Option	Description
<i>disable</i>	Ignore source selector when choosing tunnel.
<i>enable</i>	Use source selector to choose tunnel.

config vpn ipsec forticlient

Configure FortiClient policy realm.

```
config vpn ipsec forticlient
  Description: Configure FortiClient policy realm.
  edit <realm>
    set phase2name {string}
    set status [enable|disable]
    set usergroupname {string}
  next
end
```

config vpn ipsec forticlient

Parameter	Description	Type	Size
phase2name	Phase 2 tunnel name that you defined in the FortiClient dialup configuration.	string	Maximum length: 35
realm	FortiClient realm name.	string	Maximum length: 35
status	Enable/disable this FortiClient configuration.	option	-
		Option	Description
		<i>enable</i>	Enable setting.
		<i>disable</i>	Disable setting.
usergroupname	User group name for FortiClient users.	string	Maximum length: 35

config vpn ipsec manualkey

Configure IPsec manual keys.

```
config vpn ipsec manualkey
  Description: Configure IPsec manual keys.
  edit <name>
    set authentication [null|md5|...]
    set authkey {user}
    set enckey {user}
    set encryption [null|des|...]
    set interface {string}
    set local-gw {ipv4-address-any}
    set localspi {user}
    set npu-offload [enable|disable]
    set remote-gw {ipv4-address}
    set remotespi {user}
  next
end
```

config vpn ipsec manualkey

Parameter	Description	Type	Size
authentication	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>null</i>	Null.	
	<i>md5</i>	MD5.	
	<i>sha1</i>	SHA1.	
	<i>sha256</i>	SHA256.	
	<i>sha384</i>	SHA384.	
	<i>sha512</i>	SHA512.	
authkey	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified
enckey	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified
encryption	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-
	Option	Description	
	<i>null</i>	Null.	
	<i>des</i>	DES.	
	<i>3des</i>	3DES.	
	<i>aes128</i>	AES128.	
	<i>aes192</i>	AES192.	
	<i>aes256</i>	AES256.	
	<i>aria128</i>	ARIA128.	
	<i>aria192</i>	ARIA192.	
	<i>aria256</i>	ARIA256.	
	<i>seed</i>	Seed.	
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15
local-gw	Local gateway.	ipv4-address-any	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
name	IPsec tunnel name.	string	Maximum length: 35
npu-offload *	Enable/disable NPU offloading.	option	-
	Option	Description	
	<i>enable</i>	Enable NPU offloading.	
	<i>disable</i>	Disable NPU offloading.	
remote-gw	Peer gateway.	ipv4-address	Not Specified
remotespi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified

* This parameter may not exist in some models.

config vpn ipsec manualkey-interface

Configure IPsec manual keys.

```

config vpn ipsec manualkey-interface
    Description: Configure IPsec manual keys.
    edit <name>
        set addr-type [4|6]
        set auth-alg [null|md5|...]
        set auth-key {user}
        set enc-alg [null|des|...]
        set enc-key {user}
        set interface {string}
        set ip-version [4|6]
        set local-gw {ipv4-address-any}
        set local-gw6 {ipv6-address}
        set local-spi {user}
        set npu-offload [enable|disable]
        set remote-gw {ipv4-address}
        set remote-gw6 {ipv6-address}
        set remote-spi {user}
    next
end

```

config vpn ipsec manualkey-interface

Parameter	Description	Type	Size
addr-type	IP version to use for IP packets.	option	-

Parameter	Description	Type	Size

Option	Description
4	Use IPv4 addressing for IP packets.
6	Use IPv6 addressing for IP packets.

auth-alg	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-

Option	Description
<i>null</i>	null
<i>md5</i>	md5
<i>sha1</i>	sha1
<i>sha256</i>	sha256
<i>sha384</i>	sha384
<i>sha512</i>	sha512

auth-key	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified

enc-alg	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-

Option	Description
<i>null</i>	null
<i>des</i>	des
<i>3des</i>	3des
<i>aes128</i>	aes128
<i>aes192</i>	aes192
<i>aes256</i>	aes256
<i>aria128</i>	aria128
<i>aria192</i>	aria192
<i>aria256</i>	aria256
<i>seed</i>	seed

enc-key	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified

interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15

Parameter	Description	Type	Size						
ip-version	IP version to use for VPN interface.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for gateways.</td></tr><tr><td>6</td><td>Use IPv6 addressing for gateways.</td></tr></table>			Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.
	Option	Description							
	4	Use IPv4 addressing for gateways.							
6	Use IPv6 addressing for gateways.								
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address-any	Not Specified						
local-gw6	Local IPv6 address of VPN gateway.	ipv6-address	Not Specified						
local-spi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified						
name	IPsec tunnel name.	string	Maximum length: 15						
npu-offload *	Enable/disable offloading IPsec VPN manual key sessions to NPUs.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU offloading.</td></tr><tr><td><i>disable</i></td><td>Disable NPU offloading.</td></tr></table>			Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.
	Option	Description							
	<i>enable</i>	Enable NPU offloading.							
<i>disable</i>	Disable NPU offloading.								
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						
remote-spi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified						

* This parameter may not exist in some models.

config vpn ipsec phase1

Configure VPN remote gateway.

```
config vpn ipsec phase1
  Description: Configure VPN remote gateway.
  edit <name>
    set acct-verify [enable|disable]
    set add-gw-route [enable|disable]
    set add-route [disable|enable]
    set assign-ip [disable|enable]
    set assign-ip-from [range|usrgrp|...]
    set authmethod [psk|signature]
```



```

set authmethod-remote [psk|signature]
set authpasswd {password}
set authusr {string}
set authusrgrp {string}
set auto-negotiate [enable|disable]
set backup-gateway <address1>, <address2>, ...
set banner {var-string}
set cert-id-validation [enable|disable]
set certificate <name1>, <name2>, ...
set childless-ike [enable|disable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set comments {var-string}
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dhgrp {option1}, {option2}, ...
set digital-signature-auth [enable|disable]
set distance {integer}
set dns-mode [manual|auto]
set domain {string}
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set eap [enable|disable]
set eap-exclude-peergrp {string}
set eap-identity [use-id-payload|send-request]
set enforce-unique-id [disable|keep-new|...]
set esn [require|allow|...]
set fec-base {integer}
set fec-egress [enable|disable]
set fec-ingress [enable|disable]
set fec-receive-timeout {integer}
set fec-redundant {integer}
set fec-send-timeout {integer}
set forticlient-enforcement [enable|disable]
set fragmentation [enable|disable]
set fragmentation-mtu {integer}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set ha-sync-esp-seqno [enable|disable]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ike-version [1|2]
set include-local-lan [disable|enable]
set interface {string}
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-end-ip {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set end-ip {ipv4-address}
        set start-ip {ipv4-address}
    next
end

```

```

set ipv4-name {string}
set ipv4-netmask {ipv4-netmask}
set ipv4-split-exclude {string}
set ipv4-split-include {string}
set ipv4-start-ip {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
set ipv6-end-ip {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set end-ip {ipv6-address}
        set start-ip {ipv6-address}
    next
end
set ipv6-name {string}
set ipv6-prefix {integer}
set ipv6-split-exclude {string}
set ipv6-split-include {string}
set ipv6-start-ip {ipv6-address}
set keepalive {integer}
set keylife {integer}
set local-gw {ipv4-address}
set localid {string}
set localid-type [auto|fqdn|...]
set mesh-selector-type [disable|subnet|...]
set mode [aggressive|main]
set mode-cfg [disable|enable]
set nattraversal [enable|disable|...]
set negotiate-timeout {integer}
set network-id {integer}
set network-overlay [disable|enable]
set npu-offload [enable|disable]
set peer {string}
set peergrp {string}
set peerid {string}
set peertype [any|one|...]
set ppk [disable|allow|...]
set ppk-identity {string}
set ppk-secret {password-3}
set priority {integer}
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set psksecret-remote {password-3}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set remotegw-ddns {string}
set rsa-signature-format [pkcs1|pss]
set save-password [disable|enable]
set send-cert-chain [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set split-include-service {string}

```

```

set suite-b [disable|suite-b-gcm-128|...]
set type [static|dynamic|...]
set unity-support [disable|enable]
set usrgp {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
next
end

```

config vpn ipsec phase1

Parameter	Description	Type	Size						
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable verification of RADIUS accounting record.</td></tr><tr><td>disable</td><td>Disable verification of RADIUS accounting record.</td></tr></table>	Option	Description	enable	Enable verification of RADIUS accounting record.	disable	Disable verification of RADIUS accounting record.		
Option	Description								
enable	Enable verification of RADIUS accounting record.								
disable	Disable verification of RADIUS accounting record.								
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Automatically add a route to the remote gateway.</td></tr><tr><td>disable</td><td>Do not automatically add a route to the remote gateway.</td></tr></table>	Option	Description	enable	Automatically add a route to the remote gateway.	disable	Do not automatically add a route to the remote gateway.		
Option	Description								
enable	Automatically add a route to the remote gateway.								
disable	Do not automatically add a route to the remote gateway.								
add-route	Enable/disable control addition of a route to peer destination selector.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a route to destination of peer selector.</td></tr><tr><td>enable</td><td>Add route to destination of peer selector.</td></tr></table>	Option	Description	disable	Do not add a route to destination of peer selector.	enable	Add route to destination of peer selector.		
Option	Description								
disable	Do not add a route to destination of peer selector.								
enable	Add route to destination of peer selector.								
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not assign an IP address to the IPsec interface.</td></tr><tr><td>enable</td><td>Assign an IP address to the IPsec interface.</td></tr></table>	Option	Description	disable	Do not assign an IP address to the IPsec interface.	enable	Assign an IP address to the IPsec interface.		
Option	Description								
disable	Do not assign an IP address to the IPsec interface.								
enable	Assign an IP address to the IPsec interface.								
assign-ip-from	Method by which the IP address will be assigned.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>range</i>	Assign IP address from locally defined range.	
	<i>usrgrp</i>	Assign IP address via user group.	
	<i>dhcp</i>	Assign IP address via DHCP.	
	<i>name</i>	Assign IP address from firewall address or group.	
authmethod	Authentication method.	option	-
	Option	Description	
	<i>psk</i>	PSK authentication method.	
	<i>signature</i>	Signature authentication method.	
authmethod-remote	Authentication method (remote side).	option	-
	Option	Description	
	<i>psk</i>	PSK authentication method.	
	<i>signature</i>	Signature authentication method.	
authpasswd	XAuth password (max 35 characters).	password	Not Specified
authusr	XAuth user name.	string	Maximum length: 64
authusrgrp	Authentication user group.	string	Maximum length: 35
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-
	Option	Description	
	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	
	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.	
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr><tr><td><i>disable</i></td><td>Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr></table>	Option	Description	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.		
	Option	Description							
	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.							
<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.								
certificate <name>	Names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79						
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr><tr><td><i>disable</i></td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr></table>	Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).		
	Option	Description							
	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).							
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).								
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr><tr><td><i>enable</i></td><td>Enable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.		
	Option	Description							
	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.							
<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.								
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr><tr><td><i>enable</i></td><td>Enable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.		
	Option	Description							
	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.							
<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.								
comments	Comment.	var-string	Maximum length: 255						
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						
dhgrp	DH group.	option	-						

Parameter	Description	Type	Size

Option	Description
1	DH Group 1.
2	DH Group 2.
5	DH Group 5.
14	DH Group 14.
15	DH Group 15.
16	DH Group 16.
17	DH Group 17.
18	DH Group 18.
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.
27	DH Group 27.
28	DH Group 28.
29	DH Group 29.
30	DH Group 30.
31	DH Group 31.
32	DH Group 32.

digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-

Option	Description
<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).
<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).

distance	Distance for routes added by IKE (1 - 255).	integer	Minimum value: 1 Maximum value: 255

dns-mode	DNS server mode.	option	-

Option	Description
<i>manual</i>	Manually configure DNS servers.
<i>auto</i>	Use default DNS servers.

Parameter	Description	Type	Size								
domain	Instruct unity clients about the default DNS domain.	string	Maximum length: 63								
dpd	Dead Peer Detection mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Dead Peer Detection.</td></tr><tr><td><i>on-idle</i></td><td>Trigger Dead Peer Detection when IPsec is idle.</td></tr><tr><td><i>on-demand</i></td><td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td></tr></table>	Option	Description	<i>disable</i>	Disable Dead Peer Detection.	<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.	<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.		
Option	Description										
<i>disable</i>	Disable Dead Peer Detection.										
<i>on-idle</i>	Trigger Dead Peer Detection when IPsec is idle.										
<i>on-demand</i>	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.										
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10								
dpd-retryinterval	DPD retry interval.	user	Not Specified								
eap	Enable/disable IKEv2 EAP authentication.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 EAP authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.				
Option	Description										
<i>enable</i>	Enable IKEv2 EAP authentication.										
<i>disable</i>	Disable IKEv2 EAP authentication.										
eap-exclude-peergp	Peer group excluded from EAP authentication.	string	Maximum length: 35								
eap-identity	IKEv2 EAP peer identity type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-id-payload</i></td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td><i>send-request</i></td><td>Use EAP identity request to resolve peer identity.</td></tr></table>	Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.				
Option	Description										
<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.										
<i>send-request</i>	Use EAP identity request to resolve peer identity.										
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable peer ID uniqueness enforcement.</td></tr><tr><td><i>keep-new</i></td><td>Enforce peer ID uniqueness, keep new connection if collision found.</td></tr><tr><td><i>keep-old</i></td><td>Enforce peer ID uniqueness, keep old connection if collision found.</td></tr></table>	Option	Description	<i>disable</i>	Disable peer ID uniqueness enforcement.	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.		
Option	Description										
<i>disable</i>	Disable peer ID uniqueness enforcement.										
<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.										
<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.										
esn *	Extended sequence number (ESN) negotiation.	option	-								

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Require extended sequence number.</td></tr><tr><td><i>allow</i></td><td>Allow extended sequence number.</td></tr><tr><td><i>disable</i></td><td>Disable extended sequence number.</td></tr></table>	Option	Description	<i>require</i>	Require extended sequence number.	<i>allow</i>	Allow extended sequence number.	<i>disable</i>	Disable extended sequence number.		
Option	Description										
<i>require</i>	Require extended sequence number.										
<i>allow</i>	Allow extended sequence number.										
<i>disable</i>	Disable extended sequence number.										
fec-base	Number of base Forward Error Correction packets (1 - 100).	integer	Minimum value: 1 Maximum value: 100								
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forward Error Correction for egress IPsec traffic.</td></tr><tr><td><i>disable</i></td><td>Disable Forward Error Correction for egress IPsec traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.				
Option	Description										
<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.										
<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.										
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forward Error Correction for ingress IPsec traffic.</td></tr><tr><td><i>disable</i></td><td>Disable Forward Error Correction for ingress IPsec traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.				
Option	Description										
<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.										
<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.										
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets (1 - 10000).	integer	Minimum value: 1 Maximum value: 10000								
fec-redundant	Number of redundant Forward Error Correction packets (1 - 100).	integer	Minimum value: 1 Maximum value: 100								
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets (1 - 1000).	integer	Minimum value: 1 Maximum value: 1000								
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable FortiClient enforcement.	
	<i>disable</i>	Disable FortiClient enforcement.	
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-
	Option	Description	
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	
	<i>disable</i>	Disable intra-IKE fragmentation support.	
fragmentation-mtu	IKE fragmentation MTU (500 - 16000).	integer	Minimum value: 500 Maximum value: 16000
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable IKEv2 IDi group authentication.	
	<i>disable</i>	Disable IKEv2 IDi group authentication.	
group-authentication-secret	Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by a leading 0x.)	password-3	Not Specified
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-
	Option	Description	
	<i>enable</i>	Enable HA syncing of ESP sequence numbers.	
	<i>disable</i>	Disable HA syncing of ESP sequence numbers.	
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-
	Option	Description	
	<i>enable</i>	Enable IPsec tunnel idle timeout.	
	<i>disable</i>	Disable IPsec tunnel idle timeout.	

Parameter	Description	Type	Size						
idle-timeoutinterval	IPsec tunnel idle timeout in minutes (5 - 43200).	integer	Minimum value: 5 Maximum value: 43200						
ike-version	IKE protocol version.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Use IKEv1 protocol.</td></tr><tr><td>2</td><td>Use IKEv2 protocol.</td></tr></table>	Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.		
	Option	Description							
	1	Use IKEv1 protocol.							
2	Use IKEv2 protocol.								
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable local LAN access on Unity clients.</td></tr><tr><td><i>enable</i></td><td>Enable local LAN access on Unity clients.</td></tr></table>	Option	Description	<i>disable</i>	Disable local LAN access on Unity clients.	<i>enable</i>	Enable local LAN access on Unity clients.		
	Option	Description							
	<i>disable</i>	Disable local LAN access on Unity clients.							
<i>enable</i>	Enable local LAN access on Unity clients.								
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35						
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-end-ip	End of IPv4 range.	ipv4-address	Not Specified						
ipv4-name	IPv4 address name.	string	Maximum length: 79						
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified						
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79						
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79						
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified						
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified						
ipv4-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						

Parameter	Description	Type	Size
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified
ipv6-name	IPv6 address name.	string	Maximum length: 79
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800
local-gw	Local VPN gateway.	ipv4-address	Not Specified
localid	Local ID.	string	Maximum length: 63
localid-type	Local ID type.	option	-

Option	Description
<i>auto</i>	Select ID type automatically.
<i>fqdn</i>	Use fully qualified domain name.
<i>user-fqdn</i>	Use user fully qualified domain name.
<i>keyid</i>	Use key-id string.
<i>address</i>	Use local IP address.
<i>asn1dn</i>	Use ASN.1 distinguished name.

mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable.	
	<i>subnet</i>	Enable addition of matching subnet selector.	
	<i>host</i>	Enable addition of host to host selector.	
mode	ID protection mode used to establish a secure channel.	option	-
	Option	Description	
	<i>aggressive</i>	Aggressive mode.	
	<i>main</i>	Main mode.	
mode-cfg	Enable/disable configuration method.	option	-
	Option	Description	
	<i>disable</i>	Disable Configuration Method.	
	<i>enable</i>	Enable Configuration Method.	
name	IPsec remote gateway name.	string	Maximum length: 35
nattraversal	Enable/disable NAT traversal.	option	-
	Option	Description	
	<i>enable</i>	Enable IPsec NAT traversal.	
	<i>disable</i>	Disable IPsec NAT traversal.	
	<i>forced</i>	Force IPsec NAT traversal on.	
negotiate-timeout	IKE SA negotiation timeout in seconds (1 - 300).	integer	Minimum value: 1 Maximum value: 300
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255
network-overlay	Enable/disable network overlays.	option	-

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable network overlays.</td></tr><tr><td><i>enable</i></td><td>Enable network overlays.</td></tr></table>	Option	Description	<i>disable</i>	Disable network overlays.	<i>enable</i>	Enable network overlays.								
	Option	Description													
	<i>disable</i>	Disable network overlays.													
<i>enable</i>	Enable network overlays.														
npu-offload *	Enable/disable offloading NPU.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU offloading.</td></tr><tr><td><i>disable</i></td><td>Disable NPU offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.								
	Option	Description													
	<i>enable</i>	Enable NPU offloading.													
<i>disable</i>	Disable NPU offloading.														
peer	Accept this peer certificate.	string	Maximum length: 35												
peergrp	Accept this peer certificate group.	string	Maximum length: 35												
peerid	Accept this peer identity.	string	Maximum length: 255												
peertype	Accept this peer type.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer ID.</td></tr><tr><td><i>one</i></td><td>Accept this peer ID.</td></tr><tr><td><i>dialup</i></td><td>Accept peer ID in dialup group.</td></tr><tr><td><i>peer</i></td><td>Accept this peer certificate.</td></tr><tr><td><i>peergrp</i></td><td>Accept this peer certificate group.</td></tr></table>	Option	Description	<i>any</i>	Accept any peer ID.	<i>one</i>	Accept this peer ID.	<i>dialup</i>	Accept peer ID in dialup group.	<i>peer</i>	Accept this peer certificate.	<i>peergrp</i>	Accept this peer certificate group.		
	Option	Description													
	<i>any</i>	Accept any peer ID.													
	<i>one</i>	Accept this peer ID.													
	<i>dialup</i>	Accept peer ID in dialup group.													
	<i>peer</i>	Accept this peer certificate.													
<i>peergrp</i>	Accept this peer certificate group.														
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>require</i></td><td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td></tr></table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).						
	Option	Description													
	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).													
	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).													
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).														
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35												
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified												

Parameter	Description	Type	Size
priority	Priority for routes added by IKE (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
proposal	Phase1 proposal.	option	-

Option	Description
<i>des-md5</i>	des-md5
<i>des-sha1</i>	des-sha1
<i>des-sha256</i>	des-sha256
<i>des-sha384</i>	des-sha384
<i>des-sha512</i>	des-sha512
<i>3des-md5</i>	3des-md5
<i>3des-sha1</i>	3des-sha1
<i>3des-sha256</i>	3des-sha256
<i>3des-sha384</i>	3des-sha384
<i>3des-sha512</i>	3des-sha512
<i>aes128-md5</i>	aes128-md5
<i>aes128-sha1</i>	aes128-sha1
<i>aes128-sha256</i>	aes128-sha256
<i>aes128-sha384</i>	aes128-sha384
<i>aes128-sha512</i>	aes128-sha512
<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1
<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256
<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384
<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512
<i>aes192-md5</i>	aes192-md5
<i>aes192-sha1</i>	aes192-sha1
<i>aes192-sha256</i>	aes192-sha256
<i>aes192-sha384</i>	aes192-sha384
<i>aes192-sha512</i>	aes192-sha512

Parameter	Description	Type	Size

Option	Description
<i>aes256-md5</i>	aes256-md5
<i>aes256-sha1</i>	aes256-sha1
<i>aes256-sha256</i>	aes256-sha256
<i>aes256-sha384</i>	aes256-sha384
<i>aes256-sha512</i>	aes256-sha512
<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1
<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256
<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384
<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512
<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1
<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256
<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384
<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512
<i>aria128-md5</i>	aria128-md5
<i>aria128-sha1</i>	aria128-sha1
<i>aria128-sha256</i>	aria128-sha256
<i>aria128-sha384</i>	aria128-sha384
<i>aria128-sha512</i>	aria128-sha512
<i>aria192-md5</i>	aria192-md5
<i>aria192-sha1</i>	aria192-sha1
<i>aria192-sha256</i>	aria192-sha256
<i>aria192-sha384</i>	aria192-sha384
<i>aria192-sha512</i>	aria192-sha512
<i>aria256-md5</i>	aria256-md5
<i>aria256-sha1</i>	aria256-sha1
<i>aria256-sha256</i>	aria256-sha256
<i>aria256-sha384</i>	aria256-sha384
<i>aria256-sha512</i>	aria256-sha512
<i>seed-md5</i>	seed-md5

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512		
	Option	Description											
	<i>seed-sha1</i>	seed-sha1											
	<i>seed-sha256</i>	seed-sha256											
	<i>seed-sha384</i>	seed-sha384											
<i>seed-sha512</i>	seed-sha512												
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified										
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified										
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IKE SA re-authentication.</td></tr><tr><td><i>enable</i></td><td>Enable IKE SA re-authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.						
	Option	Description											
	<i>disable</i>	Disable IKE SA re-authentication.											
<i>enable</i>	Enable IKE SA re-authentication.												
rekey	Enable/disable phase1 rekey.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phase1 rekey.</td></tr><tr><td><i>disable</i></td><td>Disable phase1 rekey.</td></tr></table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.						
	Option	Description											
	<i>enable</i>	Enable phase1 rekey.											
<i>disable</i>	Disable phase1 rekey.												
remote-gw	Remote VPN gateway.	ipv4-address	Not Specified										
remotegw-ddns	Domain name of remote gateway (eg. name.DDNS.com).	string	Maximum length: 63										
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pkcs1</i></td><td>RSASSA PKCS#1 v1.5.</td></tr><tr><td><i>pss</i></td><td>RSASSA Probabilistic Signature Scheme (PSS).</td></tr></table>	Option	Description	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).						
	Option	Description											
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.											
<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).												
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-										

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable saving XAuth username and password on VPN clients.	
	<i>enable</i>	Enable saving XAuth username and password on VPN clients.	
send-cert-chain	Enable/disable sending certificate chain.	option	-
	Option	Description	
	<i>enable</i>	Enable sending certificate chain.	
	<i>disable</i>	Disable sending certificate chain.	
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-
	Option	Description	
	<i>sha1</i>	SHA1.	
	<i>sha2-256</i>	SHA2-256.	
	<i>sha2-384</i>	SHA2-384.	
	<i>sha2-512</i>	SHA2-512.	
split-include-service	Split-include services.	string	Maximum length: 79
suite-b	Use Suite-B.	option	-
	Option	Description	
	<i>disable</i>	Do not use UI suite.	
	<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.	
	<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.	
type	Remote gateway type.	option	-
	Option	Description	
	<i>static</i>	Remote VPN gateway has fixed IP address.	
	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.	
	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.	
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.	
	<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.	
usrgrp	User group name for dialup peers.	string	Maximum length: 35
wizard-type	GUI VPN Wizard Type.	option	-
	Option	Description	
	<i>custom</i>	Custom VPN configuration.	
	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.	
	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.	
	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.	
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	
	<i>static-fortigate</i>	Site to Site - FortiGate.	
	<i>dialup-fortigate</i>	Dial Up - FortiGate.	
	<i>static-cisco</i>	Site to Site - Cisco.	
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	
	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).	
	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.	
<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.		
xauthtype	XAuth type.	option	-
	Option	Description	
	<i>disable</i>	Disable.	
	<i>client</i>	Enable as client.	
	<i>pap</i>	Enable as server PAP.	
	<i>chap</i>	Enable as server CHAP.	
	<i>auto</i>	Enable as server auto.	

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified

config ipv6-exclude-range

Parameter	Description	Type	Size
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified

config vpn ipsec phase1-interface

Configure VPN remote gateway.

```
config vpn ipsec phase1-interface
  Description: Configure VPN remote gateway.
  edit <name>
    set acct-verify [enable|disable]
    set add-gw-route [enable|disable]
    set add-route [disable|enable]
    set aggregate-member [enable|disable]
    set assign-ip [disable|enable]
    set assign-ip-from [range|usrgrp|...]
    set authmethod [psk|signature]
    set authmethod-remote [psk|signature]
    set authpasswd {password}
    set authusr {string}
    set authusrgrp {string}
    set auto-discovery-forwarder [enable|disable]
    set auto-discovery-psk [enable|disable]
    set auto-discovery-receiver [enable|disable]
    set auto-discovery-sender [enable|disable]
    set auto-negotiate [enable|disable]
    set backup-gateway <address1>, <address2>, ...
```

```
set banner {var-string}
set cert-id-validation [enable|disable]
set certificate <name1>, <name2>, ...
set childless-ike [enable|disable]
set client-auto-negotiate [disable|enable]
set client-keep-alive [disable|enable]
set comments {var-string}
set default-gw {ipv4-address}
set default-gw-priority {integer}
set dhcp-ra-giaddr {ipv4-address}
set dhcp6-ra-linkaddr {ipv6-address}
set dhgrp {option1}, {option2}, ...
set digital-signature-auth [enable|disable]
set distance {integer}
set dns-mode [manual|auto]
set domain {string}
set dpd [disable|on-idle|...]
set dpd-retrycount {integer}
set dpd-retryinterval {user}
set eap [enable|disable]
set eap-exclude-peergrp {string}
set eap-identity [use-id-payload|send-request]
set encap-local-gw4 {ipv4-address}
set encap-local-gw6 {ipv6-address}
set encap-remote-gw4 {ipv4-address}
set encap-remote-gw6 {ipv6-address}
set encapsulation [none|gre|...]
set encapsulation-address [ike|ipv4|...]
set enforce-unique-id [disable|keep-new|...]
set esn [require|allow|...]
set exchange-interface-ip [enable|disable]
set exchange-ip-addr4 {ipv4-address}
set exchange-ip-addr6 {ipv6-address}
set fec-base {integer}
set fec-egress [enable|disable]
set fec-ingress [enable|disable]
set fec-receive-timeout {integer}
set fec-redundant {integer}
set fec-send-timeout {integer}
set forticlient-enforcement [enable|disable]
set fragmentation [enable|disable]
set fragmentation-mtu {integer}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set ha-sync-esp-seqno [enable|disable]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ike-version [1|2]
set include-local-lan [disable|enable]
set interface {string}
set ip-fragmentation [pre-encapsulation|post-encapsulation]
set ip-version [4|6]
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-end-ip {ipv4-address}
```

```

config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set end-ip {ipv4-address}
        set start-ip {ipv4-address}
    next
end
set ipv4-name {string}
set ipv4-netmask {ipv4-netmask}
set ipv4-split-exclude {string}
set ipv4-split-include {string}
set ipv4-start-ip {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
set ipv6-end-ip {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set end-ip {ipv6-address}
        set start-ip {ipv6-address}
    next
end
set ipv6-name {string}
set ipv6-prefix {integer}
set ipv6-split-exclude {string}
set ipv6-split-include {string}
set ipv6-start-ip {ipv6-address}
set keepalive {integer}
set keylife {integer}
set local-gw {ipv4-address}
set local-gw6 {ipv6-address}
set localid {string}
set localid-type [auto|fqdn|...]
set mesh-selector-type [disable|subnet|...]
set mode [aggressive|main]
set mode-cfg [disable|enable]
set monitor {string}
set monitor-hold-down-delay {integer}
set monitor-hold-down-time {user}
set monitor-hold-down-type [immediate|delay|...]
set monitor-hold-down-weekday [everyday|sunday|...]
set nattraversal [enable|disable|...]
set negotiate-timeout {integer}
set net-device [enable|disable]
set network-id {integer}
set network-overlay [disable|enable]
set npu-offload [enable|disable]
set passive-mode [enable|disable]
set peer {string}
set peergrp {string}
set peerid {string}
set peertype [any|one|...]
set ppk [disable|allow|...]

```

```

set ppk-identity {string}
set ppk-secret {password-3}
set priority {integer}
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set psksecret-remote {password-3}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set remote-gw6 {ipv6-address}
set remotegw-ddns {string}
set rsa-signature-format [pkcs1|pss]
set save-password [disable|enable]
set send-cert-chain [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set split-include-service {string}
set suite-b [disable|suite-b-gcm-128|...]
set tunnel-search [selectors|nexthop]
set type [static|dynamic|...]
set unity-support [disable|enable]
set usrgrp {string}
set vni {integer}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]

```

next

end

config vpn ipsec phase1-interface

Parameter	Description	Type	Size
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-
	Option	Description	
	<i>enable</i>	Enable verification of RADIUS accounting record.	
	<i>disable</i>	Disable verification of RADIUS accounting record.	
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-
	Option	Description	
	<i>enable</i>	Automatically add a route to the remote gateway.	
	<i>disable</i>	Do not automatically add a route to the remote gateway.	
add-route	Enable/disable control addition of a route to peer destination selector.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Do not add a route to destination of peer selector.	
	<i>enable</i>	Add route to destination of peer selector.	
aggregate-member	Enable/disable use as an aggregate member.	option	-
	Option	Description	
	<i>enable</i>	Enable use as an aggregate member.	
	<i>disable</i>	Disable use as an aggregate member.	
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-
	Option	Description	
	<i>disable</i>	Do not assign an IP address to the IPsec interface.	
	<i>enable</i>	Assign an IP address to the IPsec interface.	
assign-ip-from	Method by which the IP address will be assigned.	option	-
	Option	Description	
	<i>range</i>	Assign IP address from locally defined range.	
	<i>usrgrp</i>	Assign IP address via user group.	
	<i>dhcp</i>	Assign IP address via DHCP.	
	<i>name</i>	Assign IP address from firewall address or group.	
authmethod	Authentication method.	option	-
	Option	Description	
	<i>psk</i>	PSK authentication method.	
	<i>signature</i>	Signature authentication method.	
authmethod-remote	Authentication method (remote side).	option	-
	Option	Description	
	<i>psk</i>	PSK authentication method.	
	<i>signature</i>	Signature authentication method.	

Parameter	Description	Type	Size
authpasswd	XAuth password (max 35 characters).	password	Not Specified
authusr	XAuth user name.	string	Maximum length: 64
authusrgrp	Authentication user group.	string	Maximum length: 35
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-

Option	Description
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.

auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-

Option	Description
<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.
<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.

auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-

Option	Description
<i>enable</i>	Enable receiving auto-discovery short-cut messages.
<i>disable</i>	Disable receiving auto-discovery short-cut messages.

auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-

Option	Description
<i>enable</i>	Enable sending auto-discovery short-cut messages.
<i>disable</i>	Disable sending auto-discovery short-cut messages.

auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-

Option	Description
<i>enable</i>	Enable automatic initiation of IKE SA negotiation.
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.

Parameter	Description	Type	Size
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-

Option	Description
<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.
<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.

certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-

Option	Description
<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).

client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-

Option	Description
<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.
<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.

client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-

Option	Description
<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.

comments	Comment.	var-string	Maximum length: 255
default-gw	IPv4 address of default route gateway to use for traffic exiting the interface.	ipv4-address	Not Specified
default-gw-priority	Priority for default gateway route. A higher priority number signifies a less preferred route.	integer	Minimum value: 0 Maximum value: 4294967295
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
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.
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.
27	DH Group 27.
28	DH Group 28.
29	DH Group 29.

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.		
	Option	Description									
	30	DH Group 30.									
	31	DH Group 31.									
32	DH Group 32.										
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr><tr><td>disable</td><td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr></table>	Option	Description	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).	disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).				
	Option	Description									
	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).									
disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).										
distance	Distance for routes added by IKE (1 - 255).	integer	Minimum value: 1 Maximum value: 255								
dns-mode	DNS server mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>manual</td><td>Manually configure DNS servers.</td></tr><tr><td>auto</td><td>Use default DNS servers.</td></tr></table>	Option	Description	manual	Manually configure DNS servers.	auto	Use default DNS servers.				
	Option	Description									
	manual	Manually configure DNS servers.									
auto	Use default DNS servers.										
domain	Instruct unity clients about the default DNS domain.	string	Maximum length: 63								
dpd	Dead Peer Detection mode.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Dead Peer Detection.</td></tr><tr><td>on-idle</td><td>Trigger Dead Peer Detection when IPsec is idle.</td></tr><tr><td>on-demand</td><td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td></tr></table>	Option	Description	disable	Disable Dead Peer Detection.	on-idle	Trigger Dead Peer Detection when IPsec is idle.	on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.		
	Option	Description									
	disable	Disable Dead Peer Detection.									
	on-idle	Trigger Dead Peer Detection when IPsec is idle.									
on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.										
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10								
dpd-retryinterval	DPD retry interval.	user	Not Specified								
eap	Enable/disable IKEv2 EAP authentication.	option	-								

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 EAP authentication.</td></tr></table>			Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.		
	Option	Description									
	<i>enable</i>	Enable IKEv2 EAP authentication.									
<i>disable</i>	Disable IKEv2 EAP authentication.										
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35								
eap-identity	IKEv2 EAP peer identity type.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-id-payload</i></td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td><i>send-request</i></td><td>Use EAP identity request to resolve peer identity.</td></tr></table>			Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.		
	Option	Description									
	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.									
<i>send-request</i>	Use EAP identity request to resolve peer identity.										
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								
encapsulation	Enable/disable GRE/VXLAN encapsulation.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No additional encapsulation.</td></tr><tr><td><i>gre</i></td><td>GRE encapsulation.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN encapsulation.</td></tr></table>			Option	Description	<i>none</i>	No additional encapsulation.	<i>gre</i>	GRE encapsulation.	<i>vxlan</i>	VXLAN encapsulation.
	Option	Description									
	<i>none</i>	No additional encapsulation.									
<i>gre</i>	GRE encapsulation.										
<i>vxlan</i>	VXLAN encapsulation.										
encapsulation-address	Source for GRE/VXLAN tunnel address.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ike</i></td><td>Use IKE/IPsec gateway addresses.</td></tr><tr><td><i>ipv4</i></td><td>Specify separate GRE/VXLAN tunnel address.</td></tr><tr><td><i>ipv6</i></td><td>Specify separate GRE/VXLAN tunnel address.</td></tr></table>			Option	Description	<i>ike</i>	Use IKE/IPsec gateway addresses.	<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.	<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.
	Option	Description									
	<i>ike</i>	Use IKE/IPsec gateway addresses.									
	<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.									
<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.										
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable peer ID uniqueness enforcement.	
	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.	
	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.	
esn *	Extended sequence number (ESN) negotiation.	option	-
	Option	Description	
	<i>require</i>	Require extended sequence number.	
	<i>allow</i>	Allow extended sequence number.	
	<i>disable</i>	Disable extended sequence number.	
exchange-interface-ip	Enable/disable exchange of IPsec interface IP address.	option	-
	Option	Description	
	<i>enable</i>	Enable exchange of IPsec interface IP address.	
	<i>disable</i>	Disable exchange of IPsec interface IP address.	
exchange-ip-addr4	IPv4 address to exchange with peers.	ipv4-address	Not Specified
exchange-ip-addr6	IPv6 address to exchange with peers	ipv6-address	Not Specified
fec-base	Number of base Forward Error Correction packets (1 - 100).	integer	Minimum value: 1 Maximum value: 100
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-
	Option	Description	
	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.	
	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.	
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.	
	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.	
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets (1 - 10000).	integer	Minimum value: 1 Maximum value: 10000
fec-redundant	Number of redundant Forward Error Correction packets (1 - 100).	integer	Minimum value: 1 Maximum value: 100
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets (1 - 1000).	integer	Minimum value: 1 Maximum value: 1000
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-
	Option	Description	
	<i>enable</i>	Enable FortiClient enforcement.	
	<i>disable</i>	Disable FortiClient enforcement.	
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-
	Option	Description	
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	
	<i>disable</i>	Disable intra-IKE fragmentation support.	
fragmentation-mtu	IKE fragmentation MTU (500 - 16000).	integer	Minimum value: 500 Maximum value: 16000
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable IKEv2 IDi group authentication.	
	<i>disable</i>	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						
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HA syncing of ESP sequence numbers.</td></tr><tr><td>disable</td><td>Disable HA syncing of ESP sequence numbers.</td></tr></table>	Option	Description	enable	Enable HA syncing of ESP sequence numbers.	disable	Disable HA syncing of ESP sequence numbers.		
Option	Description								
enable	Enable HA syncing of ESP sequence numbers.								
disable	Disable HA syncing of ESP sequence numbers.								
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPsec tunnel idle timeout.</td></tr><tr><td>disable</td><td>Disable IPsec tunnel idle timeout.</td></tr></table>	Option	Description	enable	Enable IPsec tunnel idle timeout.	disable	Disable IPsec tunnel idle timeout.		
Option	Description								
enable	Enable IPsec tunnel idle timeout.								
disable	Disable IPsec tunnel idle timeout.								
idle-timeoutinterval	IPsec tunnel idle timeout in minutes (5 - 43200).	integer	Minimum value: 5 Maximum value: 43200						
ike-version	IKE protocol version.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Use IKEv1 protocol.</td></tr><tr><td>2</td><td>Use IKEv2 protocol.</td></tr></table>	Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.		
Option	Description								
1	Use IKEv1 protocol.								
2	Use IKEv2 protocol.								
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable local LAN access on Unity clients.</td></tr><tr><td>enable</td><td>Enable local LAN access on Unity clients.</td></tr></table>	Option	Description	disable	Disable local LAN access on Unity clients.	enable	Enable local LAN access on Unity clients.		
Option	Description								
disable	Disable local LAN access on Unity clients.								
enable	Enable local LAN access on Unity clients.								
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35						
ip-fragmentation	Determine whether IP packets are fragmented before or after IPsec encapsulation.	option	-						

Parameter	Description	Type	Size

Option	Description
<i>pre-encapsulation</i>	Fragment before IPsec encapsulation.
<i>post-encapsulation</i>	Fragment after IPsec encapsulation (RFC compliant).

ip-version	IP version to use for VPN interface.	option	-

Option	Description
4	Use IPv4 addressing for gateways.
6	Use IPv6 addressing for gateways.

ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified
ipv4-name	IPv4 address name.	string	Maximum length: 79
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified
ipv4-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-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified
ipv6-name	IPv6 address name.	string	Maximum length: 79

Parameter	Description	Type	Size
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800
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
localid	Local ID.	string	Maximum length: 63
localid-type	Local ID type.	option	-

Option	Description
<i>auto</i>	Select ID type automatically.
<i>fqdn</i>	Use fully qualified domain name.
<i>user-fqdn</i>	Use user fully qualified domain name.
<i>keyid</i>	Use key-id string.
<i>address</i>	Use local IP address.
<i>asn1dn</i>	Use ASN.1 distinguished name.

mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>subnet</i></td><td>Enable addition of matching subnet selector.</td></tr><tr><td><i>host</i></td><td>Enable addition of host to host selector.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>subnet</i>	Enable addition of matching subnet selector.	<i>host</i>	Enable addition of host to host selector.		
	Option	Description									
	<i>disable</i>	Disable.									
	<i>subnet</i>	Enable addition of matching subnet selector.									
<i>host</i>	Enable addition of host to host selector.										
mode	The ID protection mode used to establish a secure channel.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aggressive</i></td><td>Aggressive mode.</td></tr><tr><td><i>main</i></td><td>Main mode.</td></tr></table>	Option	Description	<i>aggressive</i>	Aggressive mode.	<i>main</i>	Main mode.				
	Option	Description									
	<i>aggressive</i>	Aggressive mode.									
<i>main</i>	Main mode.										
mode-cfg	Enable/disable configuration method.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Configuration Method.</td></tr><tr><td><i>enable</i></td><td>Enable Configuration Method.</td></tr></table>	Option	Description	<i>disable</i>	Disable Configuration Method.	<i>enable</i>	Enable Configuration Method.				
	Option	Description									
	<i>disable</i>	Disable Configuration Method.									
<i>enable</i>	Enable Configuration Method.										
monitor	IPsec interface as backup for primary interface.	string	Maximum length: 35								
monitor-hold-down-delay	Time to wait in seconds before recovery once primary re-establishes.	integer	Minimum value: 0 Maximum value: 31536000								
monitor-hold-down-time	Time of day at which to fail back to primary after it re-establishes.	user	Not Specified								
monitor-hold-down-type	Recovery time method when primary interface re-establishes.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediate</i></td><td>Fail back immediately after primary recovers.</td></tr><tr><td><i>delay</i></td><td>Number of seconds to delay fail back after primary recovers.</td></tr><tr><td><i>time</i></td><td>Specify a time at which to fail back after primary recovers.</td></tr></table>	Option	Description	<i>immediate</i>	Fail back immediately after primary recovers.	<i>delay</i>	Number of seconds to delay fail back after primary recovers.	<i>time</i>	Specify a time at which to fail back after primary recovers.		
	Option	Description									
	<i>immediate</i>	Fail back immediately after primary recovers.									
	<i>delay</i>	Number of seconds to delay fail back after primary recovers.									
<i>time</i>	Specify a time at which to fail back after primary recovers.										
monitor-hold-down-weekday	Day of the week to recover once primary re-establishes.	option	-								

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>everyday</i></td><td>Every Day.</td></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>	Option	Description	<i>everyday</i>	Every Day.	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.		
	Option	Description																			
	<i>everyday</i>	Every Day.																			
	<i>sunday</i>	Sunday.																			
	<i>monday</i>	Monday.																			
	<i>tuesday</i>	Tuesday.																			
	<i>wednesday</i>	Wednesday.																			
	<i>thursday</i>	Thursday.																			
	<i>friday</i>	Friday.																			
<i>saturday</i>	Saturday.																				
name	IPsec remote gateway name.	string	Maximum length: 15																		
nattraversal	Enable/disable NAT traversal.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec NAT traversal.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec NAT traversal.</td></tr><tr><td><i>forced</i></td><td>Force IPsec NAT traversal on.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec NAT traversal.	<i>disable</i>	Disable IPsec NAT traversal.	<i>forced</i>	Force IPsec NAT traversal on.												
	Option	Description																			
	<i>enable</i>	Enable IPsec NAT traversal.																			
	<i>disable</i>	Disable IPsec NAT traversal.																			
<i>forced</i>	Force IPsec NAT traversal on.																				
negotiate-timeout	IKE SA negotiation timeout in seconds (1 - 300).	integer	Minimum value: 1 Maximum value: 300																		
net-device	Enable/disable kernel device creation.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Create a kernel device for every tunnel.</td></tr><tr><td><i>disable</i></td><td>Do not create a kernel device for tunnels.</td></tr></table>	Option	Description	<i>enable</i>	Create a kernel device for every tunnel.	<i>disable</i>	Do not create a kernel device for tunnels.														
	Option	Description																			
	<i>enable</i>	Create a kernel device for every tunnel.																			
<i>disable</i>	Do not create a kernel device for tunnels.																				
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255																		
network-overlay	Enable/disable network overlays.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable network overlays.</td></tr></table>	Option	Description	<i>disable</i>	Disable network overlays.																
	Option	Description																			
<i>disable</i>	Disable network overlays.																				

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable network overlays.	
npu-offload *	Enable/disable offloading NPU.	option	-
	Option	Description	
	<i>enable</i>	Enable NPU offloading.	
	<i>disable</i>	Disable NPU offloading.	
passive-mode	Enable/disable IPsec passive mode for static tunnels.	option	-
	Option	Description	
	<i>enable</i>	Enable IPsec passive mode.	
	<i>disable</i>	Disable IPsec passive mode.	
peer	Accept this peer certificate.	string	Maximum length: 35
peergrp	Accept this peer certificate group.	string	Maximum length: 35
peerid	Accept this peer identity.	string	Maximum length: 255
peertype	Accept this peer type.	option	-
	Option	Description	
	<i>any</i>	Accept any peer ID.	
	<i>one</i>	Accept this peer ID.	
	<i>dialup</i>	Accept peer ID in dialup group.	
	<i>peer</i>	Accept this peer certificate.	
	<i>peergrp</i>	Accept this peer certificate group.	
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-
	Option	Description	
	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	
	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	
	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).	

Parameter	Description	Type	Size
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified
priority	Priority for routes added by IKE (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295
proposal	Phase1 proposal.	option	-

Option	Description
<i>des-md5</i>	des-md5
<i>des-sha1</i>	des-sha1
<i>des-sha256</i>	des-sha256
<i>des-sha384</i>	des-sha384
<i>des-sha512</i>	des-sha512
<i>3des-md5</i>	3des-md5
<i>3des-sha1</i>	3des-sha1
<i>3des-sha256</i>	3des-sha256
<i>3des-sha384</i>	3des-sha384
<i>3des-sha512</i>	3des-sha512
<i>aes128-md5</i>	aes128-md5
<i>aes128-sha1</i>	aes128-sha1
<i>aes128-sha256</i>	aes128-sha256
<i>aes128-sha384</i>	aes128-sha384
<i>aes128-sha512</i>	aes128-sha512
<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1
<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256
<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384
<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512
<i>aes192-md5</i>	aes192-md5

Parameter	Description	Type	Size

Option	Description
<i>aes192-sha1</i>	aes192-sha1
<i>aes192-sha256</i>	aes192-sha256
<i>aes192-sha384</i>	aes192-sha384
<i>aes192-sha512</i>	aes192-sha512
<i>aes256-md5</i>	aes256-md5
<i>aes256-sha1</i>	aes256-sha1
<i>aes256-sha256</i>	aes256-sha256
<i>aes256-sha384</i>	aes256-sha384
<i>aes256-sha512</i>	aes256-sha512
<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1
<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256
<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384
<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512
<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1
<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256
<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384
<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512
<i>aria128-md5</i>	aria128-md5
<i>aria128-sha1</i>	aria128-sha1
<i>aria128-sha256</i>	aria128-sha256
<i>aria128-sha384</i>	aria128-sha384
<i>aria128-sha512</i>	aria128-sha512
<i>aria192-md5</i>	aria192-md5
<i>aria192-sha1</i>	aria192-sha1
<i>aria192-sha256</i>	aria192-sha256
<i>aria192-sha384</i>	aria192-sha384
<i>aria192-sha512</i>	aria192-sha512
<i>aria256-md5</i>	aria256-md5
<i>aria256-sha1</i>	aria256-sha1

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512		
	Option	Description																			
	<i>aria256-sha256</i>	aria256-sha256																			
	<i>aria256-sha384</i>	aria256-sha384																			
	<i>aria256-sha512</i>	aria256-sha512																			
	<i>seed-md5</i>	seed-md5																			
	<i>seed-sha1</i>	seed-sha1																			
	<i>seed-sha256</i>	seed-sha256																			
	<i>seed-sha384</i>	seed-sha384																			
<i>seed-sha512</i>	seed-sha512																				
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																		
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																		
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IKE SA re-authentication.</td></tr><tr><td><i>enable</i></td><td>Enable IKE SA re-authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.														
	Option	Description																			
	<i>disable</i>	Disable IKE SA re-authentication.																			
<i>enable</i>	Enable IKE SA re-authentication.																				
rekey	Enable/disable phase1 rekey.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phase1 rekey.</td></tr><tr><td><i>disable</i></td><td>Disable phase1 rekey.</td></tr></table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.														
	Option	Description																			
	<i>enable</i>	Enable phase1 rekey.																			
<i>disable</i>	Disable phase1 rekey.																				
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified																		
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																		
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-																		

Parameter	Description	Type	Size
	Option	Description	
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.	
	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).	
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-
	Option	Description	
	<i>disable</i>	Disable saving XAuth username and password on VPN clients.	
	<i>enable</i>	Enable saving XAuth username and password on VPN clients.	
send-cert-chain	Enable/disable sending certificate chain.	option	-
	Option	Description	
	<i>enable</i>	Enable sending certificate chain.	
	<i>disable</i>	Disable sending certificate chain.	
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-
	Option	Description	
	<i>sha1</i>	SHA1.	
	<i>sha2-256</i>	SHA2-256.	
	<i>sha2-384</i>	SHA2-384.	
	<i>sha2-512</i>	SHA2-512.	
split-include-service	Split-include services.	string	Maximum length: 79
suite-b	Use Suite-B.	option	-
	Option	Description	
	<i>disable</i>	Do not use UI suite.	
	<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.	
	<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.	
tunnel-search	Tunnel search method for when the interface is shared.	option	-

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>selectors</i></td><td>Search for tunnel in selectors.</td></tr><tr><td><i>nexthop</i></td><td>Search for tunnel using nexthop.</td></tr></table>	Option	Description	<i>selectors</i>	Search for tunnel in selectors.	<i>nexthop</i>	Search for tunnel using nexthop.														
	Option	Description																			
	<i>selectors</i>	Search for tunnel in selectors.																			
<i>nexthop</i>	Search for tunnel using nexthop.																				
type	Remote gateway type.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Remote VPN gateway has fixed IP address.</td></tr><tr><td><i>dynamic</i></td><td>Remote VPN gateway has dynamic IP address.</td></tr><tr><td><i>ddns</i></td><td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td></tr></table>	Option	Description	<i>static</i>	Remote VPN gateway has fixed IP address.	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.												
	Option	Description																			
	<i>static</i>	Remote VPN gateway has fixed IP address.																			
	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.																			
<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.																				
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Cisco Unity Configuration Method Extensions.</td></tr><tr><td><i>enable</i></td><td>Enable Cisco Unity Configuration Method Extensions.</td></tr></table>	Option	Description	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.	<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.														
	Option	Description																			
	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.																			
<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.																				
usrgrp	User group name for dialup peers.	string	Maximum length: 35																		
vni	VNI of VXLAN tunnel.	integer	Minimum value: 1 Maximum value: 16777215																		
wizard-type	GUI VPN Wizard Type.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>custom</i></td><td>Custom VPN configuration.</td></tr><tr><td><i>dialup-forticlient</i></td><td>Dial Up - FortiClient Windows, Mac and Android.</td></tr><tr><td><i>dialup-ios</i></td><td>Dial Up - iPhone / iPad Native IPsec Client.</td></tr><tr><td><i>dialup-android</i></td><td>Dial Up - Android Native IPsec Client.</td></tr><tr><td><i>dialup-windows</i></td><td>Dial Up - Windows Native IPsec Client.</td></tr><tr><td><i>dialup-cisco</i></td><td>Dial Up - Cisco IPsec Client.</td></tr><tr><td><i>static-fortigate</i></td><td>Site to Site - FortiGate.</td></tr><tr><td><i>dialup-fortigate</i></td><td>Dial Up - FortiGate.</td></tr></table>	Option	Description	<i>custom</i>	Custom VPN configuration.	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	<i>static-fortigate</i>	Site to Site - FortiGate.	<i>dialup-fortigate</i>	Dial Up - FortiGate.		
	Option	Description																			
	<i>custom</i>	Custom VPN configuration.																			
	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.																			
	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.																			
	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.																			
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.																			
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.																			
<i>static-fortigate</i>	Site to Site - FortiGate.																				
<i>dialup-fortigate</i>	Dial Up - FortiGate.																				

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static-cisco</i></td><td>Site to Site - Cisco.</td></tr><tr><td><i>dialup-cisco-fw</i></td><td>Dialup Up - Cisco Firewall.</td></tr><tr><td><i>simplified-static-fortigate</i></td><td>Site to Site - FortiGate (SD-WAN).</td></tr><tr><td><i>hub-fortigate-auto-discovery</i></td><td>Hub role in a Hub-and-Spoke auto-discovery VPN.</td></tr><tr><td><i>spoke-fortigate-auto-discovery</i></td><td>Spoke role in a Hub-and-Spoke auto-discovery VPN.</td></tr></table>	Option	Description	<i>static-cisco</i>	Site to Site - Cisco.	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.		
	Option	Description													
	<i>static-cisco</i>	Site to Site - Cisco.													
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.													
	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).													
	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.													
<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.														
xauthtype	XAuth type.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>client</i></td><td>Enable as client.</td></tr><tr><td><i>pap</i></td><td>Enable as server PAP.</td></tr><tr><td><i>chap</i></td><td>Enable as server CHAP.</td></tr><tr><td><i>auto</i></td><td>Enable as server auto.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>client</i>	Enable as client.	<i>pap</i>	Enable as server PAP.	<i>chap</i>	Enable as server CHAP.	<i>auto</i>	Enable as server auto.		
	Option	Description													
	<i>disable</i>	Disable.													
	<i>client</i>	Enable as client.													
	<i>pap</i>	Enable as server PAP.													
	<i>chap</i>	Enable as server CHAP.													
<i>auto</i>	Enable as server auto.														

* This parameter may not exist in some models.

config ipv4-exclude-range

Parameter	Description	Type	Size
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified

config ipv6-exclude-range

Parameter	Description	Type	Size
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified

config vpn ipsec phase2

Configure VPN autokey tunnel.

```

config vpn ipsec phase2
    Description: Configure VPN autokey tunnel.
    edit <name>
        set add-route [phase1|enable|...]
        set auto-negotiate [enable|disable]
        set comments {var-string}
        set dhcp-ipsec [enable|disable]
        set dhgrp {option1}, {option2}, ...
        set dst-addr-type [subnet|range|...]
        set dst-end-ip {ipv4-address-any}
        set dst-end-ip6 {ipv6-address}
        set dst-name {string}
        set dst-name6 {string}
        set dst-port {integer}
        set dst-start-ip {ipv4-address-any}
        set dst-start-ip6 {ipv6-address}
        set dst-subnet {ipv4-classnet-any}
        set dst-subnet6 {ipv6-prefix}
        set encapsulation [tunnel-mode|transport-mode]
        set ipv4-df [enable|disable]
        set keepalive [enable|disable]
        set keylife-type [seconds|kbs|...]
        set keylifekbs {integer}
        set keylifeseconds {integer}
        set l2tp [enable|disable]
        set pfs [enable|disable]
        set phase1name {string}
        set proposal {option1}, {option2}, ...
        set protocol {integer}
        set replay [enable|disable]
        set route-overlap [use-old|use-new|...]
        set selector-match [exact|subset|...]
        set single-source [enable|disable]
        set src-addr-type [subnet|range|...]
        set src-end-ip {ipv4-address-any}
        set src-end-ip6 {ipv6-address}
        set src-name {string}
        set src-name6 {string}
        set src-port {integer}
        set src-start-ip {ipv4-address-any}

```

```

    set src-start-ip6 {ipv6-address}
    set src-subnet {ipv4-classnet-any}
    set src-subnet6 {ipv6-prefix}
    set use-natip [enable|disable]
next
end

```

config vpn ipsec phase2

Parameter	Description	Type	Size
add-route	Enable/disable automatic route addition.	option	-
	Option	Description	
	<i>phase1</i>	Add route according to phase1 add-route setting.	
	<i>enable</i>	Add route for remote proxy ID.	
	<i>disable</i>	Do not add route for remote proxy ID.	
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
comments	Comment.	var-string	Maximum length: 255
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
dhgrp	Phase2 DH group.	option	-
	Option	Description	
	<i>1</i>	DH Group 1.	
	<i>2</i>	DH Group 2.	
	<i>5</i>	DH Group 5.	
	<i>14</i>	DH Group 14.	
	<i>15</i>	DH Group 15.	
	<i>16</i>	DH Group 16.	

Parameter	Description	Type	Size

Option	Description
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.

dst-addr-type	Remote proxy ID type.	option	-

Option	Description
<i>subnet</i>	IPv4 subnet.
<i>range</i>	IPv4 range.
<i>ip</i>	IPv4 IP.
<i>name</i>	IPv4 firewall address or group name.

dst-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-name	Remote proxy ID name.	string	Maximum length: 79
dst-name6	Remote proxy ID name.	string	Maximum length: 79
dst-port	Quick mode destination port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535
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

Parameter	Description	Type	Size
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
encapsulation	ESP encapsulation mode.	option	-
	Option	Description	
	tunnel-mode	Use tunnel mode encapsulation.	
	transport-mode	Use transport mode encapsulation.	
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-
	Option	Description	
	enable	Set IPv4 DF.	
	disable	Reset IPv4 DF.	
keepalive	Enable/disable keep alive.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	
keylife-type	Keylife type.	option	-
	Option	Description	
	seconds	Key life in seconds.	
	kbs	Key life in kilobytes.	
	both	Key life both.	
keylifekbs	Phase2 key life in number of kilobytes of traffic (5120 - 4294967295).	integer	Minimum value: 5120 Maximum value: 4294967295
keylifeseconds	Phase2 key life in time in seconds (120 - 172800).	integer	Minimum value: 120 Maximum value: 172800
l2tp	Enable/disable L2TP over IPsec.	option	-

Parameter	Description	Type	Size																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable L2TP over IPsec.</td></tr><tr><td><i>disable</i></td><td>Disable L2TP over IPsec.</td></tr></table>	Option	Description	<i>enable</i>	Enable L2TP over IPsec.	<i>disable</i>	Disable L2TP over IPsec.																														
	Option	Description																																			
	<i>enable</i>	Enable L2TP over IPsec.																																			
<i>disable</i>	Disable L2TP over IPsec.																																				
name	IPsec tunnel name.	string	Maximum length: 35																																		
pfs	Enable/disable PFS feature.	option	-																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																														
	Option	Description																																			
	<i>enable</i>	Enable setting.																																			
<i>disable</i>	Disable setting.																																				
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 35																																		
proposal	Phase2 proposal.	option	-																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null-md5</i></td><td>null-md5</td></tr><tr><td><i>null-sha1</i></td><td>null-sha1</td></tr><tr><td><i>null-sha256</i></td><td>null-sha256</td></tr><tr><td><i>null-sha384</i></td><td>null-sha384</td></tr><tr><td><i>null-sha512</i></td><td>null-sha512</td></tr><tr><td><i>des-null</i></td><td>des-null</td></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr><tr><td><i>des-sha256</i></td><td>des-sha256</td></tr><tr><td><i>des-sha384</i></td><td>des-sha384</td></tr><tr><td><i>des-sha512</i></td><td>des-sha512</td></tr><tr><td><i>3des-null</i></td><td>3des-null</td></tr><tr><td><i>3des-md5</i></td><td>3des-md5</td></tr><tr><td><i>3des-sha1</i></td><td>3des-sha1</td></tr><tr><td><i>3des-sha256</i></td><td>3des-sha256</td></tr><tr><td><i>3des-sha384</i></td><td>3des-sha384</td></tr></table>	Option	Description	<i>null-md5</i>	null-md5	<i>null-sha1</i>	null-sha1	<i>null-sha256</i>	null-sha256	<i>null-sha384</i>	null-sha384	<i>null-sha512</i>	null-sha512	<i>des-null</i>	des-null	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-null</i>	3des-null	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384		
	Option	Description																																			
	<i>null-md5</i>	null-md5																																			
	<i>null-sha1</i>	null-sha1																																			
	<i>null-sha256</i>	null-sha256																																			
	<i>null-sha384</i>	null-sha384																																			
	<i>null-sha512</i>	null-sha512																																			
	<i>des-null</i>	des-null																																			
	<i>des-md5</i>	des-md5																																			
	<i>des-sha1</i>	des-sha1																																			
	<i>des-sha256</i>	des-sha256																																			
	<i>des-sha384</i>	des-sha384																																			
	<i>des-sha512</i>	des-sha512																																			
	<i>3des-null</i>	3des-null																																			
	<i>3des-md5</i>	3des-md5																																			
	<i>3des-sha1</i>	3des-sha1																																			
<i>3des-sha256</i>	3des-sha256																																				
<i>3des-sha384</i>	3des-sha384																																				

Parameter	Description	Type	Size

Option	Description
<i>3des-sha512</i>	3des-sha512
<i>aes128-null</i>	aes128-null
<i>aes128-md5</i>	aes128-md5
<i>aes128-sha1</i>	aes128-sha1
<i>aes128-sha256</i>	aes128-sha256
<i>aes128-sha384</i>	aes128-sha384
<i>aes128-sha512</i>	aes128-sha512
<i>aes128gcm</i>	aes128gcm
<i>aes192-null</i>	aes192-null
<i>aes192-md5</i>	aes192-md5
<i>aes192-sha1</i>	aes192-sha1
<i>aes192-sha256</i>	aes192-sha256
<i>aes192-sha384</i>	aes192-sha384
<i>aes192-sha512</i>	aes192-sha512
<i>aes256-null</i>	aes256-null
<i>aes256-md5</i>	aes256-md5
<i>aes256-sha1</i>	aes256-sha1
<i>aes256-sha256</i>	aes256-sha256
<i>aes256-sha384</i>	aes256-sha384
<i>aes256-sha512</i>	aes256-sha512
<i>aes256gcm</i>	aes256gcm
<i>chacha20poly1305</i>	chacha20poly1305
<i>aria128-null</i>	aria128-null
<i>aria128-md5</i>	aria128-md5
<i>aria128-sha1</i>	aria128-sha1
<i>aria128-sha256</i>	aria128-sha256
<i>aria128-sha384</i>	aria128-sha384
<i>aria128-sha512</i>	aria128-sha512
<i>aria192-null</i>	aria192-null

Parameter	Description	Type	Size																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria192-md5</i></td><td>aria192-md5</td></tr><tr><td><i>aria192-sha1</i></td><td>aria192-sha1</td></tr><tr><td><i>aria192-sha256</i></td><td>aria192-sha256</td></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-null</i></td><td>aria256-null</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512		
	Option	Description																																					
	<i>aria192-md5</i>	aria192-md5																																					
	<i>aria192-sha1</i>	aria192-sha1																																					
	<i>aria192-sha256</i>	aria192-sha256																																					
	<i>aria192-sha384</i>	aria192-sha384																																					
	<i>aria192-sha512</i>	aria192-sha512																																					
	<i>aria256-null</i>	aria256-null																																					
	<i>aria256-md5</i>	aria256-md5																																					
	<i>aria256-sha1</i>	aria256-sha1																																					
	<i>aria256-sha256</i>	aria256-sha256																																					
	<i>aria256-sha384</i>	aria256-sha384																																					
	<i>aria256-sha512</i>	aria256-sha512																																					
	<i>seed-null</i>	seed-null																																					
	<i>seed-md5</i>	seed-md5																																					
	<i>seed-sha1</i>	seed-sha1																																					
	<i>seed-sha256</i>	seed-sha256																																					
	<i>seed-sha384</i>	seed-sha384																																					
<i>seed-sha512</i>	seed-sha512																																						
protocol	Quick mode protocol selector (1 - 255 or 0 for all).	integer	Minimum value: 0 Maximum value: 255																																				
replay	Enable/disable replay detection.	option	-																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																
	Option	Description																																					
	<i>enable</i>	Enable setting.																																					
<i>disable</i>	Disable setting.																																						
route-overlap	Action for overlapping routes.	option	-																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-old</i></td><td>Use the old route and do not add the new route.</td></tr><tr><td><i>use-new</i></td><td>Delete the old route and add the new route.</td></tr></table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.	<i>use-new</i>	Delete the old route and add the new route.																																
	Option	Description																																					
	<i>use-old</i>	Use the old route and do not add the new route.																																					
<i>use-new</i>	Delete the old route and add the new route.																																						

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow overlapping routes.</td></tr></table>	Option	Description	<i>allow</i>	Allow overlapping routes.								
	Option	Description											
	<i>allow</i>	Allow overlapping routes.											
selector-match	Match type to use when comparing selectors.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exact</i></td><td>Match selectors exactly.</td></tr><tr><td><i>subset</i></td><td>Match selectors by subset.</td></tr><tr><td><i>auto</i></td><td>Use subset or exact match depending on selector address type.</td></tr></table>	Option	Description	<i>exact</i>	Match selectors exactly.	<i>subset</i>	Match selectors by subset.	<i>auto</i>	Use subset or exact match depending on selector address type.				
	Option	Description											
	<i>exact</i>	Match selectors exactly.											
	<i>subset</i>	Match selectors by subset.											
<i>auto</i>	Use subset or exact match depending on selector address type.												
single-source	Enable/disable single source IP restriction.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Only single source IP will be accepted.</td></tr><tr><td><i>disable</i></td><td>Source IP range will be accepted.</td></tr></table>	Option	Description	<i>enable</i>	Only single source IP will be accepted.	<i>disable</i>	Source IP range will be accepted.						
	Option	Description											
	<i>enable</i>	Only single source IP will be accepted.											
<i>disable</i>	Source IP range will be accepted.												
src-addr-type	Local proxy ID type.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subnet</i></td><td>IPv4 subnet.</td></tr><tr><td><i>range</i></td><td>IPv4 range.</td></tr><tr><td><i>ip</i></td><td>IPv4 IP.</td></tr><tr><td><i>name</i></td><td>IPv4 firewall address or group name.</td></tr></table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.	<i>ip</i>	IPv4 IP.	<i>name</i>	IPv4 firewall address or group name.		
	Option	Description											
	<i>subnet</i>	IPv4 subnet.											
	<i>range</i>	IPv4 range.											
	<i>ip</i>	IPv4 IP.											
	<i>name</i>	IPv4 firewall address or group name.											
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified										
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified										
src-name	Local proxy ID name.	string	Maximum length: 79										
src-name6	Local proxy ID name.	string	Maximum length: 79										
src-port	Quick mode source port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535										
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified										
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified										

Parameter	Description	Type	Size
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
use-natip	Enable to use the FortiGate public IP as the source selector when outbound NAT is used.	option	-

Option	Description
<i>enable</i>	Replace source selector with interface IP when using outbound NAT.
<i>disable</i>	Do not modify source selector when using outbound NAT.

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```
config vpn ipsec phase2-interface
    Description: Configure VPN autokey tunnel.
    edit <name>
        set add-route [phase1|enable|...]
        set auto-discovery-forwarder [phase1|enable|...]
        set auto-discovery-sender [phase1|enable|...]
        set auto-negotiate [enable|disable]
        set comments {var-string}
        set dhcp-ipsec [enable|disable]
        set dhgrp {option1}, {option2}, ...
        set dst-addr-type [subnet|range|...]
        set dst-end-ip {ipv4-address-any}
        set dst-end-ip6 {ipv6-address}
        set dst-name {string}
        set dst-name6 {string}
        set dst-port {integer}
        set dst-start-ip {ipv4-address-any}
        set dst-start-ip6 {ipv6-address}
        set dst-subnet {ipv4-classnet-any}
        set dst-subnet6 {ipv6-prefix}
        set encapsulation [tunnel-mode|transport-mode]
        set ipv4-df [enable|disable]
        set keepalive [enable|disable]
        set keylife-type [seconds|kbs|...]
        set keylifekbs {integer}
        set keylifeseconds {integer}
        set l2tp [enable|disable]
        set pfs [enable|disable]
        set phase1name {string}
        set proposal {option1}, {option2}, ...
        set protocol {integer}
        set replay [enable|disable]
        set route-overlap [use-old|use-new|...]
        set single-source [enable|disable]
```

```

set src-addr-type [subnet|range|...]
set src-end-ip {ipv4-address-any}
set src-end-ip6 {ipv6-address}
set src-name {string}
set src-name6 {string}
set src-port {integer}
set src-start-ip {ipv4-address-any}
set src-start-ip6 {ipv6-address}
set src-subnet {ipv4-classnet-any}
set src-subnet6 {ipv6-prefix}
next
end

```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size								
add-route	Enable/disable automatic route addition.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Add route according to phase1 add-route setting.</td></tr><tr><td><i>enable</i></td><td>Add route for remote proxy ID.</td></tr><tr><td><i>disable</i></td><td>Do not add route for remote proxy ID.</td></tr></table>	Option	Description	<i>phase1</i>	Add route according to phase1 add-route setting.	<i>enable</i>	Add route for remote proxy ID.	<i>disable</i>	Do not add route for remote proxy ID.		
Option	Description										
<i>phase1</i>	Add route according to phase1 add-route setting.										
<i>enable</i>	Add route for remote proxy ID.										
<i>disable</i>	Do not add route for remote proxy ID.										
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.</td></tr><tr><td><i>enable</i></td><td>Enable forwarding auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable forwarding auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.		
Option	Description										
<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.										
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.										
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.										
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Send short-cut messages according to the phase1 auto-discovery-sender setting.</td></tr><tr><td><i>enable</i></td><td>Enable sending auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable sending auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.		
Option	Description										
<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.										
<i>enable</i>	Enable sending auto-discovery short-cut messages.										
<i>disable</i>	Disable sending auto-discovery short-cut messages.										
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-								

Parameter	Description	Type	Size																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																
	Option	Description																																					
	<i>enable</i>	Enable setting.																																					
<i>disable</i>	Disable setting.																																						
comments	Comment.	var-string	Maximum length: 255																																				
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																
	Option	Description																																					
	<i>enable</i>	Enable setting.																																					
<i>disable</i>	Disable setting.																																						
dhgrp	Phase2 DH group.	option	-																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>DH Group 1.</td></tr><tr><td>2</td><td>DH Group 2.</td></tr><tr><td>5</td><td>DH Group 5.</td></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.		
	Option	Description																																					
	1	DH Group 1.																																					
	2	DH Group 2.																																					
	5	DH Group 5.																																					
	14	DH Group 14.																																					
	15	DH Group 15.																																					
	16	DH Group 16.																																					
	17	DH Group 17.																																					
	18	DH Group 18.																																					
	19	DH Group 19.																																					
	20	DH Group 20.																																					
	21	DH Group 21.																																					
	27	DH Group 27.																																					
	28	DH Group 28.																																					
	29	DH Group 29.																																					
	30	DH Group 30.																																					
	31	DH Group 31.																																					
32	DH Group 32.																																						
dst-addr-type	Remote proxy ID type.	option	-																																				

Parameter	Description	Type	Size

Option	Description
<i>subnet</i>	IPv4 subnet.
<i>range</i>	IPv4 range.
<i>ip</i>	IPv4 IP.
<i>name</i>	IPv4 firewall address or group name.
<i>subnet6</i>	IPv6 subnet.
<i>range6</i>	IPv6 range.
<i>ip6</i>	IPv6 IP.
<i>name6</i>	IPv6 firewall address or group name.

dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified
dst-name	Remote proxy ID name.	string	Maximum length: 79
dst-name6	Remote proxy ID name.	string	Maximum length: 79
dst-port	Quick mode destination port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535
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-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified
encapsulation	ESP encapsulation mode.	option	-

Option	Description
<i>tunnel-mode</i>	Use tunnel mode encapsulation.
<i>transport-mode</i>	Use transport mode encapsulation.

ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Set IPv4 DF.	
	<i>disable</i>	Reset IPv4 DF.	
keepalive	Enable/disable keep alive.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
keylife-type	Keylife type.	option	-
	Option	Description	
	<i>seconds</i>	Key life in seconds.	
	<i>kbs</i>	Key life in kilobytes.	
	<i>both</i>	Key life both.	
keylifekbs	Phase2 key life in number of kilobytes of traffic (5120 - 4294967295).	integer	Minimum value: 5120 Maximum value: 4294967295
keylifeseconds	Phase2 key life in time in seconds (120 - 172800).	integer	Minimum value: 120 Maximum value: 172800
l2tp	Enable/disable L2TP over IPsec.	option	-
	Option	Description	
	<i>enable</i>	Enable L2TP over IPsec.	
	<i>disable</i>	Disable L2TP over IPsec.	
name	IPsec tunnel name.	string	Maximum length: 35
pfs	Enable/disable PFS feature.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15
proposal	Phase2 proposal.	option	-

Option	Description
<i>null-md5</i>	null-md5
<i>null-sha1</i>	null-sha1
<i>null-sha256</i>	null-sha256
<i>null-sha384</i>	null-sha384
<i>null-sha512</i>	null-sha512
<i>des-null</i>	des-null
<i>des-md5</i>	des-md5
<i>des-sha1</i>	des-sha1
<i>des-sha256</i>	des-sha256
<i>des-sha384</i>	des-sha384
<i>des-sha512</i>	des-sha512
<i>3des-null</i>	3des-null
<i>3des-md5</i>	3des-md5
<i>3des-sha1</i>	3des-sha1
<i>3des-sha256</i>	3des-sha256
<i>3des-sha384</i>	3des-sha384
<i>3des-sha512</i>	3des-sha512
<i>aes128-null</i>	aes128-null
<i>aes128-md5</i>	aes128-md5
<i>aes128-sha1</i>	aes128-sha1
<i>aes128-sha256</i>	aes128-sha256
<i>aes128-sha384</i>	aes128-sha384
<i>aes128-sha512</i>	aes128-sha512
<i>aes128gcm</i>	aes128gcm
<i>aes192-null</i>	aes192-null
<i>aes192-md5</i>	aes192-md5

Parameter	Description	Type	Size

Option	Description
<i>aes192-sha1</i>	aes192-sha1
<i>aes192-sha256</i>	aes192-sha256
<i>aes192-sha384</i>	aes192-sha384
<i>aes192-sha512</i>	aes192-sha512
<i>aes256-null</i>	aes256-null
<i>aes256-md5</i>	aes256-md5
<i>aes256-sha1</i>	aes256-sha1
<i>aes256-sha256</i>	aes256-sha256
<i>aes256-sha384</i>	aes256-sha384
<i>aes256-sha512</i>	aes256-sha512
<i>aes256gcm</i>	aes256gcm
<i>chacha20poly1305</i>	chacha20poly1305
<i>aria128-null</i>	aria128-null
<i>aria128-md5</i>	aria128-md5
<i>aria128-sha1</i>	aria128-sha1
<i>aria128-sha256</i>	aria128-sha256
<i>aria128-sha384</i>	aria128-sha384
<i>aria128-sha512</i>	aria128-sha512
<i>aria192-null</i>	aria192-null
<i>aria192-md5</i>	aria192-md5
<i>aria192-sha1</i>	aria192-sha1
<i>aria192-sha256</i>	aria192-sha256
<i>aria192-sha384</i>	aria192-sha384
<i>aria192-sha512</i>	aria192-sha512
<i>aria256-null</i>	aria256-null
<i>aria256-md5</i>	aria256-md5
<i>aria256-sha1</i>	aria256-sha1
<i>aria256-sha256</i>	aria256-sha256
<i>aria256-sha384</i>	aria256-sha384

Parameter	Description	Type	Size																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512		
	Option	Description																	
	<i>aria256-sha512</i>	aria256-sha512																	
	<i>seed-null</i>	seed-null																	
	<i>seed-md5</i>	seed-md5																	
	<i>seed-sha1</i>	seed-sha1																	
	<i>seed-sha256</i>	seed-sha256																	
	<i>seed-sha384</i>	seed-sha384																	
<i>seed-sha512</i>	seed-sha512																		
protocol	Quick mode protocol selector (1 - 255 or 0 for all).	integer	Minimum value: 0 Maximum value: 255																
replay	Enable/disable replay detection.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.												
	Option	Description																	
	<i>enable</i>	Enable setting.																	
<i>disable</i>	Disable setting.																		
route-overlap	Action for overlapping routes.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-old</i></td><td>Use the old route and do not add the new route.</td></tr><tr><td><i>use-new</i></td><td>Delete the old route and add the new route.</td></tr><tr><td><i>allow</i></td><td>Allow overlapping routes.</td></tr></table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.	<i>use-new</i>	Delete the old route and add the new route.	<i>allow</i>	Allow overlapping routes.										
	Option	Description																	
	<i>use-old</i>	Use the old route and do not add the new route.																	
	<i>use-new</i>	Delete the old route and add the new route.																	
<i>allow</i>	Allow overlapping routes.																		
single-source	Enable/disable single source IP restriction.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Only single source IP will be accepted.</td></tr><tr><td><i>disable</i></td><td>Source IP range will be accepted.</td></tr></table>	Option	Description	<i>enable</i>	Only single source IP will be accepted.	<i>disable</i>	Source IP range will be accepted.												
	Option	Description																	
	<i>enable</i>	Only single source IP will be accepted.																	
<i>disable</i>	Source IP range will be accepted.																		
src-addr-type	Local proxy ID type.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subnet</i></td><td>IPv4 subnet.</td></tr><tr><td><i>range</i></td><td>IPv4 range.</td></tr></table>	Option	Description	<i>subnet</i>	IPv4 subnet.	<i>range</i>	IPv4 range.												
	Option	Description																	
	<i>subnet</i>	IPv4 subnet.																	
<i>range</i>	IPv4 range.																		

Parameter	Description	Type	Size

Option	Description
<i>ip</i>	IPv4 IP.
<i>name</i>	IPv4 firewall address or group name.
<i>subnet6</i>	IPv6 subnet.
<i>range6</i>	IPv6 range.
<i>ip6</i>	IPv6 IP.
<i>name6</i>	IPv6 firewall address or group name.

src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified
src-name	Local proxy ID name.	string	Maximum length: 79
src-name6	Local proxy ID name.	string	Maximum length: 79
src-port	Quick mode source port (1 - 65535 or 0 for all).	integer	Minimum value: 0 Maximum value: 65535
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-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified

config vpn l2tp

Configure L2TP.

```

config vpn l2tp
    Description: Configure L2TP.
    set compress [enable|disable]
    set eip {ipv4-address}
    set enforce-ipsec [enable|disable]
    set sip {ipv4-address}
    set status [enable|disable]
    set usrgrp {string}
end

```

config vpn l2tp

Parameter	Description	Type	Size
compress	Enable/disable data compression.	option	-
	Option	Description	
	<i>enable</i>	Enable compress	
	<i>disable</i>	Disable compress	
eip	End IP.	ipv4-address	Not Specified
enforce-ipsec	Enable/disable IPsec enforcement.	option	-
	Option	Description	
	<i>enable</i>	Enable enforce-ipsec	
	<i>disable</i>	Disable enforce-ipsec	
sip	Start IP.	ipv4-address	Not Specified
status	Enable/disable FortiGate as a L2TP gateway.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
usrgrp	User group.	string	Maximum length: 35

config vpn ocvpn

Configure Overlay Controller VPN settings.

```
config vpn ocvpn
  Description: Configure Overlay Controller VPN settings.
  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 assign-ip [enable|disable]
      set ipv4-end-ip {ipv4-address}
      set ipv4-start-ip {ipv4-address}
      set name {string}
```

```

config subnets
    Description: Internal subnets to register with OCVPN service.
    edit <id>
        set interface {string}
        set subnet {ipv4-classnet-any}
        set type [subnet|interface]
    next
end
next
end
set poll-interval {integer}
set role [spoke|primary-hub|...]
set status [enable|disable]
end

```

config vpn ocvpn

Parameter	Description	Type	Size						
auto-discovery	Enable/disable auto-discovery shortcuts.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ADVPN auto-discovery shortcuts.</td></tr><tr><td><i>disable</i></td><td>Disable ADVPN auto-discovery shortcuts.</td></tr></table>	Option	Description	<i>enable</i>	Enable ADVPN auto-discovery shortcuts.	<i>disable</i>	Disable ADVPN auto-discovery shortcuts.		
Option	Description								
<i>enable</i>	Enable ADVPN auto-discovery shortcuts.								
<i>disable</i>	Disable ADVPN auto-discovery shortcuts.								
eap	Enable/disable EAP client authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAP client authentication.</td></tr><tr><td><i>disable</i></td><td>Disable EAP client authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAP client authentication.	<i>disable</i>	Disable EAP client authentication.		
Option	Description								
<i>enable</i>	Enable EAP client authentication.								
<i>disable</i>	Disable EAP client authentication.								
eap-users	EAP authentication user group.	string	Maximum length: 35						
nat	Enable/disable inter-overlay source NAT.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inter-overlay source NAT.</td></tr><tr><td><i>disable</i></td><td>Disable inter-overlay source NAT.</td></tr></table>	Option	Description	<i>enable</i>	Enable inter-overlay source NAT.	<i>disable</i>	Disable inter-overlay source NAT.		
Option	Description								
<i>enable</i>	Enable inter-overlay source NAT.								
<i>disable</i>	Disable inter-overlay source NAT.								
poll-interval	Overlay Controller VPN polling interval.	integer	Minimum value: 30 Maximum value: 120						
role	Set device role.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>spoke</i>	Register device as static spoke.	
	<i>primary-hub</i>	Register device as primary hub.	
	<i>secondary-hub</i>	Register device as secondary hub.	
status	Enable/disable Overlay Controller cloud assisted VPN.	option	-
	Option	Description	
	<i>enable</i>	Enable Overlay Controller VPN.	
	<i>disable</i>	Disable Overlay Controller VPN.	

config overlays

Parameter	Description	Type	Size
assign-ip	Enable/disable client address assignment.	option	-
	Option	Description	
	<i>enable</i>	Enable client IPv4 address assignment.	
	<i>disable</i>	Disable client IPv4 address assignment.	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
ipv4-end-ip	End of client IPv4 range.	ipv4-address	Not Specified
ipv4-start-ip	Start of client IPv4 range.	ipv4-address	Not Specified
name	Overlay name.	string	Maximum length: 63

config subnets

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

Parameter	Description	Type	Size
interface	LAN interface.	string	Maximum length: 15
subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified
type	Subnet type.	option	-

Option	Description
<i>subnet</i>	Configure participating subnet IP and mask.
<i>interface</i>	Configure participating LAN interface.

config vpn pptp

Configure PPTP.

```
config vpn pptp
    Description: Configure PPTP.
    set eip {ipv4-address}
    set ip-mode [range|usrgrp]
    set local-ip {ipv4-address}
    set sip {ipv4-address}
    set status [enable|disable]
    set usrgrp {string}
end
```

config vpn pptp

Parameter	Description	Type	Size
eip	End IP.	ipv4-address	Not Specified
ip-mode	IP assignment mode for PPTP client.	option	-

Option	Description
<i>range</i>	PPTP client IP from manual config (range from sip to eip).
<i>usrgrp</i>	PPTP client IP from user-group defined server.

local-ip	Local IP to be used for peer's remote IP.	ipv4-address	Not Specified
sip	Start IP.	ipv4-address	Not Specified
status	Enable/disable FortiGate as a PPTP gateway.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
usrgrp	User group.	string	Maximum length: 35

config vpn ssl settings

Configure SSL VPN.

```

config vpn ssl settings
    Description: Configure SSL VPN.
    set algorithm [high|medium|...]
    set auth-session-check-source-ip [enable|disable]
    set auth-timeout {integer}
    config authentication-rule
        Description: Authentication rule for SSL VPN.
        edit <id>
            set auth [any|local|...]
            set cipher [any|high|...]
            set client-cert [enable|disable]
            set groups <name1>, <name2>, ...
            set portal {string}
            set realm {string}
            set source-address <name1>, <name2>, ...
            set source-address-negate [enable|disable]
            set source-address6 <name1>, <name2>, ...
            set source-address6-negate [enable|disable]
            set source-interface <name1>, <name2>, ...
            set user-peer {string}
            set users <name1>, <name2>, ...
        next
    end
    set auto-tunnel-static-route [enable|disable]
    set banned-cipher {option1}, {option2}, ...
    set check-referer [enable|disable]
    set default-portal {string}
    set deflate-compression-level {integer}
    set deflate-min-data-size {integer}
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-suffix {var-string}
    set dtls-hello-timeout {integer}
    set dtls-max-proto-ver [dtls1-0|dtls1-2]
    set dtls-min-proto-ver [dtls1-0|dtls1-2]
    set dtls-tunnel [enable|disable]
    set encode-2f-sequence [enable|disable]
    set force-two-factor-auth [enable|disable]
    set header-x-forwarded-for [pass|add|...]

```



```

set hsts-include-subdomains [enable|disable]
set http-compression [enable|disable]
set http-only-cookie [enable|disable]
set http-request-body-timeout {integer}
set http-request-header-timeout {integer}
set https-redirect [enable|disable]
set idle-timeout {integer}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-wins-server1 {ipv6-address}
set ipv6-wins-server2 {ipv6-address}
set login-attempt-limit {integer}
set login-block-time {integer}
set login-timeout {integer}
set port {integer}
set port-precedence [enable|disable]
set reqclientcert [enable|disable]
set route-source-interface [enable|disable]
set servercert {string}
set source-address <name1>, <name2>, ...
set source-address-negate [enable|disable]
set source-address6 <name1>, <name2>, ...
set source-address6-negate [enable|disable]
set source-interface <name1>, <name2>, ...
set ssl-client-renegotiation [disable|enable]
set ssl-insert-empty-fragment [enable|disable]
set ssl-max-proto-ver [tls1-0|tls1-1|...]
set ssl-min-proto-ver [tls1-0|tls1-1|...]
set tlsv1-0 [enable|disable]
set tlsv1-1 [enable|disable]
set tlsv1-2 [enable|disable]
set tlsv1-3 [enable|disable]
set tunnel-connect-without-reauth [enable|disable]
set tunnel-ip-pools <name1>, <name2>, ...
set tunnel-ipv6-pools <name1>, <name2>, ...
set tunnel-user-session-timeout {integer}
set unsafe-legacy-renegotiation [enable|disable]
set url-obscuration [enable|disable]
set user-peer {string}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
set x-content-type-options [enable|disable]

```

end

config vpn ssl settings

Parameter	Description	Type	Size
algorithm	Force the SSL-VPN security level. High allows only high. Medium allows medium and high. Low allows any.	option	-

Parameter	Description	Type	Size																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High algorithms.</td></tr><tr><td>medium</td><td>High and medium algorithms.</td></tr><tr><td>default</td><td>default</td></tr><tr><td>low</td><td>All algorithms.</td></tr></table>	Option	Description	high	High algorithms.	medium	High and medium algorithms.	default	default	low	All algorithms.								
	Option	Description																	
	high	High algorithms.																	
	medium	High and medium algorithms.																	
	default	default																	
low	All algorithms.																		
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable checking of source IP for authentication session.</td></tr><tr><td>disable</td><td>Disable checking of source IP for authentication session.</td></tr></table>	Option	Description	enable	Enable checking of source IP for authentication session.	disable	Disable checking of source IP for authentication session.												
	Option	Description																	
	enable	Enable checking of source IP for authentication session.																	
disable	Disable checking of source IP for authentication session.																		
auth-timeout	SSL-VPN authentication timeout (1 - 259200 sec (3 days), 0 for no timeout).	integer	Minimum value: 0 Maximum value: 259200																
auto-tunnel-static-route	Enable to auto-create static routes for the SSL-VPN tunnel IP addresses.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.												
	Option	Description																	
	enable	Enable setting.																	
disable	Disable setting.																		
banned-cipher	Select one or more cipher technologies that cannot be used in SSL-VPN negotiations.	option	-																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>RSA</td><td>Ban the use of cipher suites using RSA key.</td></tr><tr><td>DHE</td><td>Ban the use of cipher suites using authenticated ephemeral DH key agreement.</td></tr><tr><td>ECDHE</td><td>Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.</td></tr><tr><td>DSS</td><td>Ban the use of cipher suites using DSS authentication.</td></tr><tr><td>ECDSA</td><td>Ban the use of cipher suites using ECDSA authentication.</td></tr><tr><td>AES</td><td>Ban the use of cipher suites using either 128 or 256 bit AES.</td></tr><tr><td>AESGCM</td><td>Ban the use of cipher suites AES in Galois Counter Mode (GCM).</td></tr></table>	Option	Description	RSA	Ban the use of cipher suites using RSA key.	DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.	ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.	DSS	Ban the use of cipher suites using DSS authentication.	ECDSA	Ban the use of cipher suites using ECDSA authentication.	AES	Ban the use of cipher suites using either 128 or 256 bit AES.	AESGCM	Ban the use of cipher suites AES in Galois Counter Mode (GCM).		
	Option	Description																	
	RSA	Ban the use of cipher suites using RSA key.																	
	DHE	Ban the use of cipher suites using authenticated ephemeral DH key agreement.																	
	ECDHE	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.																	
	DSS	Ban the use of cipher suites using DSS authentication.																	
	ECDSA	Ban the use of cipher suites using ECDSA authentication.																	
AES	Ban the use of cipher suites using either 128 or 256 bit AES.																		
AESGCM	Ban the use of cipher suites AES in Galois Counter Mode (GCM).																		

Parameter	Description	Type	Size

Option	Description
<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.
<i>3DES</i>	Ban the use of cipher suites using triple DES
<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.
<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.
<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.
<i>STATIC</i>	Ban the use of cipher suites using static keys.

check-referer	Enable/disable verification of referer field in HTTP request header.	option	-

Option	Description
<i>enable</i>	Enable verification of referer field in HTTP request header.
<i>disable</i>	Disable verification of referer field in HTTP request header.

default-portal	Default SSL VPN portal.	string	Maximum length: 35
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 (200 - 65535 bytes).	integer	Minimum value: 200 Maximum value: 65535
dns-server1	DNS server 1.	ipv4-address	Not Specified
dns-server2	DNS server 2.	ipv4-address	Not Specified
dns-suffix	DNS suffix used for SSL-VPN clients.	var-string	Maximum length: 253
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout (10 - 60 sec, default = 10).	integer	Minimum value: 10 Maximum value: 60
dtls-max-protocol-ver	DTLS maximum protocol version.	option	-

Option	Description
<i>dtls1-0</i>	DTLS version 1.0.

Parameter	Description	Type	Size
	Option	Description	
	<i>dtls1-2</i>	DTLS version 1.2.	
dtls-min-protocol-ver	DTLS minimum protocol version.	option	-
	Option	Description	
	<i>dtls1-0</i>	DTLS version 1.0.	
	<i>dtls1-2</i>	DTLS version 1.2.	
dtls-tunnel	Enable DTLS to prevent eavesdropping, tampering, or message forgery.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
encode-2f-sequence	Encode \2F sequence to forward slash in URLs.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
force-two-factor-auth	Enable only PKI users with two-factor authentication for SSL-VPNs.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
http-compression	Enable to allow HTTP compression over SSL-VPN tunnels.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
http-only-cookie	Enable/disable SSL-VPN support for HttpOnly cookies.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
http-request-body-timeout	SSL-VPN session is disconnected if an HTTP request body is not received within this time (1 - 60 sec, default = 20).	integer	Minimum value: 0 Maximum value: 4294967295
http-request-header-timeout	SSL-VPN session is disconnected if an HTTP request header is not received within this time (1 - 60 sec, default = 20).	integer	Minimum value: 0 Maximum value: 4294967295
https-redirect	Enable/disable redirect of port 80 to SSL-VPN port.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
idle-timeout	SSL VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified

Parameter	Description	Type	Size						
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						
login-attempt-limit	SSL VPN maximum login attempt times before block (0 - 10, default = 2, 0 = no limit).	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 (0 - 86400 sec, default = 60).	integer	Minimum value: 0 Maximum value: 4294967295						
login-timeout	SSLVPN maximum login timeout (10 - 180 sec, default = 30).	integer	Minimum value: 10 Maximum value: 180						
port	SSL-VPN access port (1 - 65535).	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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
reqclientcert	Enable to require client certificates for all SSL-VPN users.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
route-source-interface	Enable to allow SSL-VPN sessions to bypass routing and bind to the incoming interface.	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
servercert	Name of the server certificate to be used for SSL-VPNs.	string	Maximum length: 35						
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79						
source-address-negate	Enable/disable negated source address match.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
source-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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
source-interface <name>	SSL VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35						
ssl-client-renegotiation	Enable to allow client renegotiation by the server if the tunnel goes down.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Abort any SSL connection that attempts to renegotiate.</td></tr><tr><td><i>enable</i></td><td>Allow a SSL client to renegotiate.</td></tr></table>	Option	Description	<i>disable</i>	Abort any SSL connection that attempts to renegotiate.	<i>enable</i>	Allow a SSL client to renegotiate.		
Option	Description								
<i>disable</i>	Abort any SSL connection that attempts to renegotiate.								
<i>enable</i>	Allow a SSL client to renegotiate.								
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-						

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
ssl-max-protocol-ver	SSL maximum protocol version.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls1-0</i></td><td>TLS version 1.0.</td></tr><tr><td><i>tls1-1</i></td><td>TLS version 1.1.</td></tr><tr><td><i>tls1-2</i></td><td>TLS version 1.2.</td></tr><tr><td><i>tls1-3</i></td><td>TLS version 1.3.</td></tr></table>	Option	Description	<i>tls1-0</i>	TLS version 1.0.	<i>tls1-1</i>	TLS version 1.1.	<i>tls1-2</i>	TLS version 1.2.	<i>tls1-3</i>	TLS version 1.3.		
	Option	Description											
	<i>tls1-0</i>	TLS version 1.0.											
	<i>tls1-1</i>	TLS version 1.1.											
	<i>tls1-2</i>	TLS version 1.2.											
<i>tls1-3</i>	TLS version 1.3.												
ssl-min-protocol-ver	SSL minimum protocol version.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls1-0</i></td><td>TLS version 1.0.</td></tr><tr><td><i>tls1-1</i></td><td>TLS version 1.1.</td></tr><tr><td><i>tls1-2</i></td><td>TLS version 1.2.</td></tr><tr><td><i>tls1-3</i></td><td>TLS version 1.3.</td></tr></table>	Option	Description	<i>tls1-0</i>	TLS version 1.0.	<i>tls1-1</i>	TLS version 1.1.	<i>tls1-2</i>	TLS version 1.2.	<i>tls1-3</i>	TLS version 1.3.		
	Option	Description											
	<i>tls1-0</i>	TLS version 1.0.											
	<i>tls1-1</i>	TLS version 1.1.											
	<i>tls1-2</i>	TLS version 1.2.											
<i>tls1-3</i>	TLS version 1.3.												
tlsv1-0	tlsv1-0	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
tlsv1-1	tlsv1-1	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												
tlsv1-2	tlsv1-2	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description											
	<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.												

Parameter	Description	Type	Size						
tlsv1-3	tlsv1-3	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
tunnel-connect-without-reauth	Enable/disable tunnel connection without re-authorization if previous connection dropped.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable tunnel connection without re-authorization.</td></tr><tr><td><i>disable</i></td><td>Disable tunnel connection without re-authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable tunnel connection without re-authorization.	<i>disable</i>	Disable tunnel connection without re-authorization.		
	Option	Description							
	<i>enable</i>	Enable tunnel connection without re-authorization.							
<i>disable</i>	Disable tunnel connection without re-authorization.								
tunnel-ip-pools <name>	Names of the IPv4 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79						
tunnel-ipv6-pools <name>	Names of the IPv6 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79						
tunnel-user-session-timeout	Time out value to clean up user session after tunnel connection is dropped (1 - 255 sec, default=30).	integer	Minimum value: 1 Maximum value: 255						
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
url-obscuration	Enable to obscure the host name of the URL of the web browser display.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description							
	<i>enable</i>	Enable setting.							
<i>disable</i>	Disable setting.								
user-peer	Name of user peer.	string	Maximum length: 35						
wins-server1	WINS server 1.	ipv4-address	Not Specified						

Parameter	Description	Type	Size
wins-server2	WINS server 2.	ipv4-address	Not Specified
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config authentication-rule

Parameter	Description	Type	Size
auth	SSL VPN authentication method restriction.	option	-

Option	Description
<i>any</i>	Any
<i>local</i>	Local
<i>radius</i>	RADIUS
<i>tacacs+</i>	TACACS+
<i>ldap</i>	LDAP

cipher	SSL VPN cipher strength.	option	-

Option	Description
<i>any</i>	Any cipher strength.
<i>high</i>	High cipher strength (>= 168 bits).
<i>medium</i>	Medium cipher strength (>= 128 bits).

client-cert	Enable/disable SSL VPN client certificate restrictive.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

groups <name>	User groups. Group name.	string	Maximum length: 79

Parameter	Description	Type	Size						
id	ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295						
portal	SSL VPN portal.	string	Maximum length: 35						
realm	SSL VPN realm.	string	Maximum length: 35						
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79						
source-address-negate	Enable/disable negated source address match.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>			Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79						
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>			Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
source-interface <name>	SSL VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35						
user-peer	Name of user peer.	string	Maximum length: 35						
users <name>	User name. User name.	string	Maximum length: 79						

config vpn ssl web host-check-software

SSL-VPN host check software.

```
config vpn ssl web host-check-software
  Description: SSL-VPN host check software.
  edit <name>
    config check-item-list
      Description: Check item list.
      edit <id>
        set action [require|deny]
        set md5s <id1>, <id2>, ...
        set target {string}
        set type [file|registry|...]
        set version {string}
      next
    end
    set guid {user}
    set os-type [windows|macos]
    set type [av|fw]
    set version {string}
  next
end
```

config vpn ssl web host-check-software

Parameter	Description	Type	Size
guid	Globally unique ID.	user	Not Specified
name	Name.	string	Maximum length: 63
os-type	OS type.	option	-
		Option	Description
		<i>windows</i>	Microsoft Windows operating system.
		<i>macos</i>	Apple MacOS operating system.
type	Type.	option	-
		Option	Description
		<i>av</i>	AntiVirus.
		<i>fw</i>	Firewall.
version	Version.	string	Maximum length: 35

config check-item-list

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	require	Require.	
	deny	Deny.	
id	ID (0 - 4294967295).	integer	Minimum value: 0 Maximum value: 65535
md5s <id>	MD5 checksum. Hex string of MD5 checksum.	string	Maximum length: 32
target	Target.	string	Maximum length: 255
type	Type.	option	-
	Option	Description	
	file	File.	
	registry	Registry.	
	process	Process.	
version	Version.	string	Maximum length: 35

config vpn ssl web portal

Portal.

```
config vpn ssl web portal
  Description: Portal.
  edit <name>
    set allow-user-access {option1}, {option2}, ...
    set auto-connect [enable|disable]
    config bookmark-group
      Description: Portal bookmark group.
      edit <name>
        config bookmarks
          Description: Bookmark table.
          edit <name>
            set additional-params {var-string}
            set apptype [ftp|rdp|...]
            set description {var-string}
```

```

        set folder {var-string}
        config form-data
            Description: Form data.
            edit <name>
                set value {var-string}
            next
        end
        set host {var-string}
        set listening-port {integer}
        set load-balancing-info {var-string}
        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set remote-port {integer}
        set security [rdp|nla|...]
        set server-layout [de-de-qwertz|en-gb-qwerty|...]
        set show-status-window [enable|disable]
        set sso [disable|static|...]
        set sso-credential [sslvpn-login|alternative]
        set sso-credential-sent-once [enable|disable]
        set sso-password {password}
        set sso-username {var-string}
        set url {var-string}
    next
end
next
end
set custom-lang {string}
set customize-forticlient-download-url [enable|disable]
set display-bookmark [enable|disable]
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set dns-server1 {ipv4-address}
set dns-server2 {ipv4-address}
set dns-suffix {var-string}
set exclusive-routing [enable|disable]
set forticlient-download [enable|disable]
set forticlient-download-method [direct|ssl-vpn]
set heading {string}
set hide-sso-credential [enable|disable]
set host-check [none|av|...]
set host-check-interval {integer}
set host-check-policy <name1>, <name2>, ...
set ip-mode [range|user-group]
set ip-pools <name1>, <name2>, ...
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-exclusive-routing [enable|disable]
set ipv6-pools <name1>, <name2>, ...
set ipv6-service-restriction [enable|disable]
set ipv6-split-tunneling [enable|disable]
set ipv6-split-tunneling-routing-address <name1>, <name2>, ...
set ipv6-tunnel-mode [enable|disable]

```

```

set ipv6-wins-server1 {ipv6-address}
set ipv6-wins-server2 {ipv6-address}
set keep-alive [enable|disable]
set limit-user-logins [enable|disable]
set mac-addr-action [allow|deny]
set mac-addr-check [enable|disable]
config mac-addr-check-rule
    Description: Client MAC address check rule.
    edit <name>
        set mac-addr-list <addr1>, <addr2>, ...
        set mac-addr-mask {integer}
    next
end
set macos-forticlient-download-url {var-string}
set os-check [enable|disable]
config os-check-list
    Description: SSL VPN OS checks. Read-only.
    edit <name>
        set action [deny|allow|...]
        set latest-patch-level {user}
        set tolerance {integer}
    next
end
set redir-url {var-string}
set save-password [enable|disable]
set service-restriction [enable|disable]
set skip-check-for-browser [enable|disable]
set skip-check-for-unsupported-os [enable|disable]
set smb-max-version [smbv1|smbv2|...]
set smb-min-version [smbv1|smbv2|...]
set smb-ntlmv1-auth [enable|disable]
set smbv1 [enable|disable]
config split-dns
    Description: Split DNS for SSL VPN.
    edit <id>
        set dns-server1 {ipv4-address}
        set dns-server2 {ipv4-address}
        set domains {var-string}
        set ipv6-dns-server1 {ipv6-address}
        set ipv6-dns-server2 {ipv6-address}
    next
end
set split-tunneling [enable|disable]
set split-tunneling-routing-address <name1>, <name2>, ...
set theme [blue|green|...]
set transform-backward-slashes [enable|disable]
set tunnel-mode [enable|disable]
set use-sdwan [enable|disable]
set user-bookmark [enable|disable]
set user-group-bookmark [enable|disable]
set web-mode [enable|disable]
set windows-forticlient-download-url {var-string}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
next
end

```

config vpn ssl web portal

Parameter	Description	Type	Size																								
allow-user-access	Allow user access to SSL-VPN applications.	option	-																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>web</td><td>HTTP/HTTPS access.</td></tr><tr><td>ftp</td><td>FTP access.</td></tr><tr><td>smb</td><td>SMB/CIFS access.</td></tr><tr><td>sftp</td><td>SFTP access.</td></tr><tr><td>telnet</td><td>TELNET access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>vnc</td><td>VNC access.</td></tr><tr><td>rdp</td><td>RDP access.</td></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>citrix</td><td>CITRIX access.</td></tr><tr><td>portforward</td><td>Port Forward access.</td></tr></table>	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.		
	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.																										
auto-connect	Enable/disable automatic connect by client when system is up.	option	-																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																				
	Option	Description																									
	enable	Enable setting.																									
disable	Disable setting.																										
custom-lang	Change the web portal display language. Overrides config system global set language. You can use config system custom-language and execute system custom-language to add custom language files.	string	Maximum length: 35																								
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																				
	Option	Description																									
	enable	Enable setting.																									
disable	Disable setting.																										
display-bookmark	Enable to display the web portal bookmark widget.	option	-																								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
display-connection-tools	Enable to display the web portal connection tools widget.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
display-history	Enable to display the web portal user login history widget.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
display-status	Enable to display the web portal status widget.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
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
exclusive-routing	Enable/disable all traffic go through tunnel only.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
forticlient-download	Enable/disable download option for FortiClient.	option	-

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
	Option	Description													
	<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.														
forticlient-download-method	FortiClient download method.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>direct</i></td><td>Download via direct link.</td></tr><tr><td><i>ssl-vpn</i></td><td>Download via SSL-VPN.</td></tr></table>	Option	Description	<i>direct</i>	Download via direct link.	<i>ssl-vpn</i>	Download via SSL-VPN.								
	Option	Description													
	<i>direct</i>	Download via direct link.													
<i>ssl-vpn</i>	Download via SSL-VPN.														
heading	Web portal heading message.	string	Maximum length: 31												
hide-sso-credential	Enable to prevent SSO credential being sent to client.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
	Option	Description													
	<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.														
host-check	Type of host checking performed on endpoints.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No host checking.</td></tr><tr><td><i>av</i></td><td>AntiVirus software recognized by the Windows Security Center.</td></tr><tr><td><i>fw</i></td><td>Firewall software recognized by the Windows Security Center.</td></tr><tr><td><i>av-fw</i></td><td>AntiVirus and firewall software recognized by the Windows Security Center.</td></tr><tr><td><i>custom</i></td><td>Custom.</td></tr></table>	Option	Description	<i>none</i>	No host checking.	<i>av</i>	AntiVirus software recognized by the Windows Security Center.	<i>fw</i>	Firewall software recognized by the Windows Security Center.	<i>av-fw</i>	AntiVirus and firewall software recognized by the Windows Security Center.	<i>custom</i>	Custom.		
	Option	Description													
	<i>none</i>	No host checking.													
	<i>av</i>	AntiVirus software recognized by the Windows Security Center.													
	<i>fw</i>	Firewall software recognized by the Windows Security Center.													
	<i>av-fw</i>	AntiVirus and firewall software recognized by the Windows Security Center.													
<i>custom</i>	Custom.														
host-check-interval	Periodic host check interval. Value of 0 means disabled and host checking only happens when the endpoint connects.	integer	Minimum value: 120 Maximum value: 259200												
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												

Parameter	Description	Type	Size

ip-mode	Method by which users of this SSL-VPN tunnel obtain IP addresses.	option	-

Option	Description
<i>range</i>	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.
<i>user-group</i>	Use IP the addresses associated with individual users or user groups (usually from external auth servers).

ip-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. 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-exclusive-routing	Enable/disable all IPv6 traffic go through tunnel only.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

ipv6-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string	Maximum length: 79

ipv6-service-restriction	Enable/disable IPv6 tunnel service restriction.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

ipv6-split-tunneling	Enable/disable IPv6 split tunneling.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

Parameter	Description	Type	Size						
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-tunnel-mode	Enable/disable IPv6 SSL-VPN tunnel mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified						
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified						
keep-alive	Enable/disable automatic reconnect for FortiClient connections.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
limit-user-logins	Enable to limit each user to one SSL-VPN session at a time.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description								
enable	Enable setting.								
disable	Disable setting.								
mac-addr-action	Client MAC address action.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow connection when client MAC address is matched.</td></tr><tr><td>deny</td><td>Deny connection when client MAC address is matched.</td></tr></table>	Option	Description	allow	Allow connection when client MAC address is matched.	deny	Deny connection when client MAC address is matched.		
Option	Description								
allow	Allow connection when client MAC address is matched.								
deny	Deny connection when client MAC address is matched.								
mac-addr-check	Enable/disable MAC address host checking.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023
name	Portal name.	string	Maximum length: 35
os-check	Enable to let the FortiGate decide action based on client OS.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
redir-url	Client login redirect URL.	var-string	Maximum length: 255
save-password	Enable/disable FortiClient saving the user's password.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
service-restriction	Enable/disable tunnel service restriction.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
skip-check-for-browser	Enable to skip host check for browser support.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size
skip-check-for-unsupported-os	Enable to skip host check if client OS does not support it.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
smb-max-version	SMB maximum client protocol version.	option	-
	Option	Description	
	<i>smbv1</i>	SMB version 1.	
	<i>smbv2</i>	SMB version 2.	
	<i>smbv3</i>	SMB version 3.	
smb-min-version	SMB minimum client protocol version.	option	-
	Option	Description	
	<i>smbv1</i>	SMB version 1.	
	<i>smbv2</i>	SMB version 2.	
	<i>smbv3</i>	SMB version 3.	
smb-ntlmv1-auth	Enable support of NTLMv1 for Samba authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
smbv1	smbv1	option	-
	Option	Description	
	<i>enable</i>	enable	
	<i>disable</i>	disable	
split-tunneling	Enable/disable IPv4 split tunneling.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.										
Option	Description														
<i>disable</i>	Disable setting.														
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												
theme	Web portal color scheme.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>blue</i></td><td>Light blue theme.</td></tr><tr><td><i>green</i></td><td>Green theme.</td></tr><tr><td><i>neutrino</i></td><td>Neutrino theme.</td></tr><tr><td><i>melongene</i></td><td>Melongene theme (eggplant color).</td></tr><tr><td><i>mariner</i></td><td>Mariner theme (dark blue color).</td></tr></table>	Option	Description	<i>blue</i>	Light blue theme.	<i>green</i>	Green theme.	<i>neutrino</i>	Neutrino theme.	<i>melongene</i>	Melongene theme (eggplant color).	<i>mariner</i>	Mariner theme (dark blue color).		
Option	Description														
<i>blue</i>	Light blue theme.														
<i>green</i>	Green theme.														
<i>neutrino</i>	Neutrino theme.														
<i>melongene</i>	Melongene theme (eggplant color).														
<i>mariner</i>	Mariner theme (dark blue color).														
transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
Option	Description														
<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.														
tunnel-mode	Enable/disable IPv4 SSL-VPN tunnel mode.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
Option	Description														
<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.														
use-sdwan	Use SD-WAN rules to get output interface.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.								
Option	Description														
<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.														
user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-												

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
web-mode	Enable/disable SSL VPN web mode.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023
wins-server1	IPv4 WINS server 1.	ipv4-address	Not Specified
wins-server2	IPv4 WINS server 1.	ipv4-address	Not Specified

config bookmark-group

Parameter	Description	Type	Size
name	Bookmark group name.	string	Maximum length: 35

config bookmarks

Parameter	Description	Type	Size
additional-params	Additional parameters.	var-string	Maximum length: 128
apptype	Application type.	option	-

Parameter	Description	Type	Size

Option	Description
<i>ftp</i>	FTP.
<i>rdp</i>	RDP.
<i>sftp</i>	SFTP.
<i>smb</i>	SMB/CIFS.
<i>ssh</i>	SSH.
<i>telnet</i>	Telnet.
<i>vnc</i>	VNC.
<i>web</i>	HTTP/HTTPS.

description	Description.	var-string	Maximum length: 128
folder	Network shared file folder parameter.	var-string	Maximum length: 128
host	Host name/IP parameter.	var-string	Maximum length: 128
listening-port	Listening port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511
logon-password	Logon password.	password	Not Specified
logon-user	Logon user.	var-string	Maximum length: 35
name	Bookmark name.	string	Maximum length: 35
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511

Parameter	Description	Type	Size																												
preconnection-id	The numeric ID of the RDP source (0-2147483648).	integer	Minimum value: 0 Maximum value: 2147483648																												
remote-port	Remote port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535																												
security	Security mode for RDP connection.	option	-																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr></table>	Option	Description	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.	<i>any</i>	Allow the server to choose the type of security.																				
	Option	Description																													
	<i>rdp</i>	Standard RDP encryption.																													
	<i>nla</i>	Network Level Authentication.																													
	<i>tls</i>	TLS encryption.																													
<i>any</i>	Allow the server to choose the type of security.																														
server-layout	Server side keyboard layout.	option	-																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>de-de-qwertz</i></td><td>German (qwertz).</td></tr><tr><td><i>en-gb-qwerty</i></td><td>English (UK).</td></tr><tr><td><i>en-us-qwerty</i></td><td>English (US).</td></tr><tr><td><i>es-es-qwerty</i></td><td>Spanish.</td></tr><tr><td><i>fr-ca-qwerty</i></td><td>Canadian French (qwerty).</td></tr><tr><td><i>fr-fr-azerty</i></td><td>French (azerty).</td></tr><tr><td><i>fr-ch-qwertz</i></td><td>Swiss French (qwertz).</td></tr><tr><td><i>it-it-qwerty</i></td><td>Italian.</td></tr><tr><td><i>ja-jp-qwerty</i></td><td>Japanese.</td></tr><tr><td><i>pt-br-qwerty</i></td><td>Portuguese/Brazilian.</td></tr><tr><td><i>sv-se-qwerty</i></td><td>Swedish.</td></tr><tr><td><i>tr-tr-qwerty</i></td><td>Turkish.</td></tr><tr><td><i>failsafe</i></td><td>Unknown keyboard.</td></tr></table>	Option	Description	<i>de-de-qwertz</i>	German (qwertz).	<i>en-gb-qwerty</i>	English (UK).	<i>en-us-qwerty</i>	English (US).	<i>es-es-qwerty</i>	Spanish.	<i>fr-ca-qwerty</i>	Canadian French (qwerty).	<i>fr-fr-azerty</i>	French (azerty).	<i>fr-ch-qwertz</i>	Swiss French (qwertz).	<i>it-it-qwerty</i>	Italian.	<i>ja-jp-qwerty</i>	Japanese.	<i>pt-br-qwerty</i>	Portuguese/Brazilian.	<i>sv-se-qwerty</i>	Swedish.	<i>tr-tr-qwerty</i>	Turkish.	<i>failsafe</i>	Unknown keyboard.		
	Option	Description																													
	<i>de-de-qwertz</i>	German (qwertz).																													
	<i>en-gb-qwerty</i>	English (UK).																													
	<i>en-us-qwerty</i>	English (US).																													
	<i>es-es-qwerty</i>	Spanish.																													
	<i>fr-ca-qwerty</i>	Canadian French (qwerty).																													
	<i>fr-fr-azerty</i>	French (azerty).																													
	<i>fr-ch-qwertz</i>	Swiss French (qwertz).																													
	<i>it-it-qwerty</i>	Italian.																													
	<i>ja-jp-qwerty</i>	Japanese.																													
	<i>pt-br-qwerty</i>	Portuguese/Brazilian.																													
<i>sv-se-qwerty</i>	Swedish.																														
<i>tr-tr-qwerty</i>	Turkish.																														
<i>failsafe</i>	Unknown keyboard.																														
show-status-window	Enable/disable showing of status window.	option	-																												

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
sso	Single Sign-On.	option	-
	Option	Description	
	<i>disable</i>	Disable SSO.	
	<i>static</i>	Static SSO.	
	<i>auto</i>	Auto SSO.	
sso-credential	Single sign-on credentials.	option	-
	Option	Description	
	<i>sslvpn-login</i>	SSL-VPN login.	
	<i>alternative</i>	Alternative.	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-
	Option	Description	
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	
	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.	
sso-password	SSO password.	password	Not Specified
sso-username	SSO user name.	var-string	Maximum length: 35
url	URL parameter.	var-string	Maximum length: 128

config form-data

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 35
value	Value.	var-string	Maximum length: 63

config mac-addr-check-rule

Parameter	Description	Type	Size
mac-addr-list <addr>	Client MAC address list. Client MAC address.	mac-address	Not Specified
mac-addr-mask	Client MAC address mask.	integer	Minimum value: 1 Maximum value: 48
name	Client MAC address check rule name.	string	Maximum length: 35

config os-check-list

Parameter	Description	Type	Size								
action	OS check options.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Deny all OS versions.</td></tr><tr><td><i>allow</i></td><td>Allow any OS version.</td></tr><tr><td><i>check-up-to-date</i></td><td>Verify OS is up-to-date.</td></tr></table>	Option	Description	<i>deny</i>	Deny all OS versions.	<i>allow</i>	Allow any OS version.	<i>check-up-to-date</i>	Verify OS is up-to-date.		
	Option	Description									
	<i>deny</i>	Deny all OS versions.									
	<i>allow</i>	Allow any OS version.									
	<i>check-up-to-date</i>	Verify OS is up-to-date.									
latest-patch-level	Latest OS patch level.	user	Not Specified								
name	Name.	string	Maximum length: 35								
tolerance	OS patch level tolerance.	integer	Minimum value: 0 Maximum value: 65535								

config split-dns

Parameter	Description	Type	Size
dns-server1	DNS server 1.	ipv4-address	Not Specified
dns-server2	DNS server 2.	ipv4-address	Not Specified
domains	Split DNS domains used for SSL-VPN clients separated by comma(.).	var-string	Maximum length: 1024

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967294
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 realm

Realm.

```
config vpn ssl web realm
    Description: Realm.
    edit <url-path>
        set login-page {var-string}
        set max-concurrent-user {integer}
        set virtual-host {var-string}
    next
end
```

config vpn ssl web realm

Parameter	Description	Type	Size
login-page	Replacement HTML for SSL-VPN login page.	var-string	Maximum length: 32768
max-concurrent-user	Maximum concurrent users (0 - 65535, 0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535
url-path	URL path to access SSL-VPN login page.	string	Maximum length: 35
virtual-host	Virtual host name for realm.	var-string	Maximum length: 255

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>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set additional-params {var-string}
        set apptype [ftp|rdp|...]
        set description {var-string}
        set folder {var-string}
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
        set host {var-string}
        set listening-port {integer}
        set load-balancing-info {var-string}
        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set remote-port {integer}
        set security [rdp|nla|...]
        set server-layout [de-de-qwertz|en-gb-qwerty|...]
        set show-status-window [enable|disable]
        set sso [disable|static|...]
        set sso-credential [sslvpn-login|alternative]
        set sso-credential-sent-once [enable|disable]
        set sso-password {password}
        set sso-username {var-string}
        set url {var-string}
      next
    end
    set custom-lang {string}
  next
end

```

config vpn ssl web user-bookmark

Parameter	Description	Type	Size
custom-lang	Personal language.	string	Maximum length: 35
name	User and group name.	string	Maximum length: 101

config bookmarks

Parameter	Description	Type	Size
additional-params	Additional parameters.	var-string	Maximum length: 128
apptype	Application type.	option	-
	Option	Description	
	<i>ftp</i>	FTP.	
	<i>rdp</i>	RDP.	
	<i>sftp</i>	SFTP.	
	<i>smb</i>	SMB/CIFS.	
	<i>ssh</i>	SSH.	
	<i>telnet</i>	Telnet.	
	<i>vnc</i>	VNC.	
	<i>web</i>	HTTP/HTTPS.	
description	Description.	var-string	Maximum length: 128
folder	Network shared file folder parameter.	var-string	Maximum length: 128
host	Host name/IP parameter.	var-string	Maximum length: 128
listening-port	Listening port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511
logon-password	Logon password.	password	Not Specified
logon-user	Logon user.	var-string	Maximum length: 35
name	Bookmark name.	string	Maximum length: 35
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511
preconnection-id	The numeric ID of the RDP source (0-2147483648).	integer	Minimum value: 0 Maximum value: 2147483648
remote-port	Remote port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535
security	Security mode for RDP connection.	option	-

Option	Description
<i>rdp</i>	Standard RDP encryption.
<i>nla</i>	Network Level Authentication.
<i>tls</i>	TLS encryption.
<i>any</i>	Allow the server to choose the type of security.

server-layout	Server side keyboard layout.	option	-

Option	Description
<i>de-de-qwertz</i>	German (qwertz).
<i>en-gb-qwerty</i>	English (UK).
<i>en-us-qwerty</i>	English (US).
<i>es-es-qwerty</i>	Spanish.
<i>fr-ca-qwerty</i>	Canadian French (qwerty).
<i>fr-fr-azerty</i>	French (azerty).
<i>fr-ch-qwertz</i>	Swiss French (qwertz).
<i>it-it-qwerty</i>	Italian.
<i>ja-jp-qwerty</i>	Japanese.
<i>pt-br-qwerty</i>	Portuguese/Brazilian.
<i>sv-se-qwerty</i>	Swedish.
<i>tr-tr-qwerty</i>	Turkish.
<i>failsafe</i>	Unknown keyboard.

Parameter	Description	Type	Size
show-status-window	Enable/disable showing of status window.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
sso	Single Sign-On.	option	-
	Option	Description	
	<i>disable</i>	Disable SSO.	
	<i>static</i>	Static SSO.	
	<i>auto</i>	Auto SSO.	
sso-credential	Single sign-on credentials.	option	-
	Option	Description	
	<i>sslvpn-login</i>	SSL-VPN login.	
	<i>alternative</i>	Alternative.	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-
	Option	Description	
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	
	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.	
sso-password	SSO password.	password	Not Specified
sso-username	SSO user name.	var-string	Maximum length: 35
url	URL parameter.	var-string	Maximum length: 128

config form-data

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 35
value	Value.	var-string	Maximum length: 63

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 additional-params {var-string}
        set apptype [ftp|rdp|...]
        set description {var-string}
        set folder {var-string}
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
        set host {var-string}
        set listening-port {integer}
        set load-balancing-info {var-string}
        set logon-password {password}
        set logon-user {var-string}
        set port {integer}
        set preconnection-blob {var-string}
        set preconnection-id {integer}
        set remote-port {integer}
        set security [rdp|nla|...]
        set server-layout [de-de-qwertz|en-gb-qwerty|...]
        set show-status-window [enable|disable]
        set sso [disable|static|...]
        set sso-credential [sslvpn-login|alternative]
        set sso-credential-sent-once [enable|disable]
        set sso-password {password}
        set sso-username {var-string}
        set url {var-string}
      next
    end
  next
end
```

config vpn ssl web user-group-bookmark

Parameter	Description	Type	Size
name	Group name.	string	Maximum length: 64

config bookmarks

Parameter	Description	Type	Size
additional-params	Additional parameters.	var-string	Maximum length: 128
apptype	Application type.	option	-
	Option	Description	
	<i>ftp</i>	FTP.	
	<i>rdp</i>	RDP.	
	<i>sftp</i>	SFTP.	
	<i>smb</i>	SMB/CIFS.	
	<i>ssh</i>	SSH.	
	<i>telnet</i>	Telnet.	
	<i>vnc</i>	VNC.	
	<i>web</i>	HTTP/HTTPS.	
description	Description.	var-string	Maximum length: 128
folder	Network shared file folder parameter.	var-string	Maximum length: 128
host	Host name/IP parameter.	var-string	Maximum length: 128
listening-port	Listening port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511
logon-password	Logon password.	password	Not Specified
logon-user	Logon user.	var-string	Maximum length: 35
name	Bookmark name.	string	Maximum length: 35
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511
preconnection-id	The numeric ID of the RDP source (0-2147483648).	integer	Minimum value: 0 Maximum value: 2147483648
remote-port	Remote port (0 - 65535).	integer	Minimum value: 0 Maximum value: 65535
security	Security mode for RDP connection.	option	-

Option	Description
<i>rdp</i>	Standard RDP encryption.
<i>nla</i>	Network Level Authentication.
<i>tls</i>	TLS encryption.
<i>any</i>	Allow the server to choose the type of security.

server-layout	Server side keyboard layout.	option	-

Option	Description
<i>de-de-qwertz</i>	German (qwertz).
<i>en-gb-qwerty</i>	English (UK).
<i>en-us-qwerty</i>	English (US).
<i>es-es-qwerty</i>	Spanish.
<i>fr-ca-qwerty</i>	Canadian French (qwerty).
<i>fr-fr-azerty</i>	French (azerty).
<i>fr-ch-qwertz</i>	Swiss French (qwertz).
<i>it-it-qwerty</i>	Italian.
<i>ja-jp-qwerty</i>	Japanese.
<i>pt-br-qwerty</i>	Portuguese/Brazilian.
<i>sv-se-qwerty</i>	Swedish.
<i>tr-tr-qwerty</i>	Turkish.
<i>failsafe</i>	Unknown keyboard.

Parameter	Description	Type	Size
show-status-window	Enable/disable showing of status window.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
sso	Single Sign-On.	option	-
	Option	Description	
	<i>disable</i>	Disable SSO.	
	<i>static</i>	Static SSO.	
	<i>auto</i>	Auto SSO.	
sso-credential	Single sign-on credentials.	option	-
	Option	Description	
	<i>sslvpn-login</i>	SSL-VPN login.	
	<i>alternative</i>	Alternative.	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-
	Option	Description	
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	
	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.	
sso-password	SSO password.	password	Not Specified
sso-username	SSO user name.	var-string	Maximum length: 35
url	URL parameter.	var-string	Maximum length: 128

config form-data

Parameter	Description	Type	Size
name	Name.	string	Maximum length: 35
value	Value.	var-string	Maximum length: 63

waf

This section includes syntax for the following commands:

- [config waf main-class on page 1454](#)
- [config waf profile on page 1454](#)
- [config waf signature on page 1479](#)
- [config waf sub-class on page 1479](#)

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
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Main signature class name.	string	Maximum length: 127

config waf profile

Web application firewall configuration.

```
config waf profile
  Description: Web application firewall configuration.
  edit <name>
    config address-list
      Description: Black address list and white address list.
      set blocked-address <name1>, <name2>, ...
      set blocked-log [enable|disable]
```

```

        set severity [high|medium|...]
        set status [enable|disable]
        set trusted-address <name1>, <name2>, ...
    end
    set comment {var-string}
    config constraint
        Description: WAF HTTP protocol restrictions.
        config content-length
            Description: HTTP content length in request.
            set action [allow|block]
            set length {integer}
            set log [enable|disable]
            set severity [high|medium|...]
            set status [enable|disable]
        end
        config exception
            Description: HTTP constraint exception.
            edit <id>
                set address {string}
                set content-length [enable|disable]
                set header-length [enable|disable]
                set hostname [enable|disable]
                set line-length [enable|disable]
                set malformed [enable|disable]
                set max-cookie [enable|disable]
                set max-header-line [enable|disable]
                set max-range-segment [enable|disable]
                set max-url-param [enable|disable]
                set method [enable|disable]
                set param-length [enable|disable]
                set pattern {string}
                set regex [enable|disable]
                set url-param-length [enable|disable]
                set version [enable|disable]
            end
        next
    end
    config header-length
        Description: HTTP header length in request.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config hostname
        Description: Enable/disable hostname check.
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config line-length
        Description: HTTP line length in request.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]

```

```

        set severity [high|medium|...]
        set status [enable|disable]
    end
    config malformed
        Description: Enable/disable malformed HTTP request check.
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config max-cookie
        Description: Maximum number of cookies in HTTP request.
        set action [allow|block]
        set log [enable|disable]
        set max-cookie {integer}
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config max-header-line
        Description: Maximum number of HTTP header line.
        set action [allow|block]
        set log [enable|disable]
        set max-header-line {integer}
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config max-range-segment
        Description: Maximum number of range segments in HTTP range line.
        set action [allow|block]
        set log [enable|disable]
        set max-range-segment {integer}
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config max-url-param
        Description: Maximum number of parameters in URL.
        set action [allow|block]
        set log [enable|disable]
        set max-url-param {integer}
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config method
        Description: Enable/disable HTTP method check.
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config param-length
        Description: Maximum length of parameter in URL, HTTP POST request or HTTP
body.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]

```



```

        set status [enable|disable]
    end
    config url-param-length
        Description: Maximum length of parameter in URL.
        set action [allow|block]
        set length {integer}
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
    config version
        Description: Enable/disable HTTP version check.
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
        set status [enable|disable]
    end
end
set extended-log [enable|disable]
set external [disable|enable]
config method
    Description: Method restriction.
    set default-allowed-methods {option1}, {option2}, ...
    set log [enable|disable]
    config method-policy
        Description: HTTP method policy.
        edit <id>
            set address {string}
            set allowed-methods {option1}, {option2}, ...
            set pattern {string}
            set regex [enable|disable]
        next
    end
    set severity [high|medium|...]
    set status [enable|disable]
end
config signature
    Description: WAF signatures.
    set credit-card-detection-threshold {integer}
    config custom-signature
        Description: Custom signature.
        edit <name>
            set action [allow|block|...]
            set case-sensitivity [disable|enable]
            set direction [request|response]
            set log [enable|disable]
            set pattern {string}
            set severity [high|medium|...]
            set status [enable|disable]
            set target {option1}, {option2}, ...
        next
    end
    set disabled-signature <id1>, <id2>, ...
    set disabled-sub-class <id1>, <id2>, ...
    config main-class
        Description: Main signature class. Read-only.

```

```

        edit <id>
            set action [allow|block|...]
            set log [enable|disable]
            set severity [high|medium|...]
            set status [enable|disable]
        next
    end
end
config url-access
    Description: URL access list
    edit <id>
        config access-pattern
            Description: URL access pattern.
            edit <id>
                set negate [enable|disable]
                set pattern {string}
                set regex [enable|disable]
                set srcaddr {string}
            next
        end
        set action [bypass|permit|...]
        set address {string}
        set log [enable|disable]
        set severity [high|medium|...]
    next
end
next
end

```

config waf profile

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 1023
extended-log	Enable/disable extended logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
external	Disable/Enable external HTTP Inspection.	option	-
	Option	Description	
	<i>disable</i>	Disable external inspection.	
	<i>enable</i>	Enable external inspection.	
name	WAF Profile name.	string	Maximum length: 35

config address-list

Parameter	Description	Type	Size								
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79								
blocked-log	Enable/disable logging on blocked addresses.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
severity	Severity.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr><tr><td><i>low</i></td><td>Low severity.</td></tr></table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.		
Option	Description										
<i>high</i>	High severity.										
<i>medium</i>	Medium severity.										
<i>low</i>	Low severity.										
status	Status.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79								

config content-length

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	

Parameter	Description	Type	Size
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
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.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	

config exception

Parameter	Description	Type	Size
address	Host address.	string	Maximum length: 79
content-length	HTTP content length in request.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
header-length	HTTP header length in request.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size
hostname	Enable/disable hostname check.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
id	Exception ID.	integer	Minimum value: 0 Maximum value: 4294967295
line-length	HTTP line length in request.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
malformed	Enable/disable malformed HTTP request check.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-cookie	Maximum number of cookies in HTTP request.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-header-line	Maximum number of HTTP header line.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-range-segment	Maximum number of range segments in HTTP range line.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-url-param	Maximum number of parameters in URL.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
method	Enable/disable HTTP method check.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
pattern	URL pattern.	string	Maximum length: 511
regex	Enable/disable regular expression based pattern match.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
url-param-length	Maximum length of parameter in URL.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
version	Enable/disable HTTP version check.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config header-length

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config hostname

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config line-length

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config malformed

Parameter	Description	Type	Size						
action	Action.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>block</i></td><td>Block.</td></tr></table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.		
Option	Description								
<i>allow</i>	Allow.								
<i>block</i>	Block.								
log	Enable/disable logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
severity	Severity.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr></table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.		
Option	Description								
<i>high</i>	High severity.								
<i>medium</i>	Medium severity.								

Parameter	Description	Type	Size
	Option	Description	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config max-cookie

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config max-header-line

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config max-range-segment

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config max-url-param

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	

Parameter	Description	Type	Size
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config method

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config param-length

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
length	Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config url-param-length

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config version

Parameter	Description	Type	Size
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.	
status	Enable/disable the constraint.	option	-
	Option	Description	
	enable	Enable setting.	
	disable	Disable setting.	

config method

Parameter	Description	Type	Size
default-allowed-methods	Methods.	option	-
	Option	Description	
	<i>get</i>	HTTP GET method.	
	<i>post</i>	HTTP POST method.	
	<i>put</i>	HTTP PUT method.	
	<i>head</i>	HTTP HEAD method.	

Parameter	Description	Type	Size
	Option	Description	
	<i>connect</i>	HTTP CONNECT method.	
	<i>trace</i>	HTTP TRACE method.	
	<i>options</i>	HTTP OPTIONS method.	
	<i>delete</i>	HTTP DELETE method.	
	<i>others</i>	Other HTTP methods.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity	
	<i>medium</i>	medium severity	
	<i>low</i>	low severity	
status	Status.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config method-policy

Parameter	Description	Type	Size
address	Host address.	string	Maximum length: 79
allowed-methods	Allowed Methods.	option	-
	Option	Description	
	<i>get</i>	HTTP GET method.	
	<i>post</i>	HTTP POST method.	

Parameter	Description	Type	Size

Option	Description
<i>put</i>	HTTP PUT method.
<i>head</i>	HTTP HEAD method.
<i>connect</i>	HTTP CONNECT method.
<i>trace</i>	HTTP TRACE method.
<i>options</i>	HTTP OPTIONS method.
<i>delete</i>	HTTP DELETE method.
<i>others</i>	Other HTTP methods.

id	HTTP method policy ID.	integer	Minimum value: 0 Maximum value: 4294967295
pattern	URL pattern.	string	Maximum length: 511
regex	Enable/disable regular expression based pattern match.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config signature

Parameter	Description	Type	Size

credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 Maximum value: 128
disabled-signature <id>	Disabled signatures Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295

config custom-signature

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
	<i>erase</i>	Erase credit card numbers.	
case-sensitivity	Case sensitivity in pattern.	option	-
	Option	Description	
	<i>disable</i>	Case insensitive in pattern.	
	<i>enable</i>	Case sensitive in pattern.	
direction	Traffic direction.	option	-
	Option	Description	
	<i>request</i>	Match HTTP request.	
	<i>response</i>	Match HTTP response.	
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
name	Signature name.	string	Maximum length: 35
pattern	Match pattern.	string	Maximum length: 511
severity	Severity.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Status.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
target	Match HTTP target.	option	-
	Option	Description	
	<i>arg</i>	HTTP arguments.	
	<i>arg-name</i>	Names of HTTP arguments.	
	<i>req-body</i>	HTTP request body.	
	<i>req-cookie</i>	HTTP request cookies.	
	<i>req-cookie-name</i>	HTTP request cookie names.	
	<i>req-filename</i>	HTTP request file name.	
	<i>req-header</i>	HTTP request headers.	
	<i>req-header-name</i>	HTTP request header names.	
	<i>req-raw-uri</i>	Raw URI of HTTP request.	
	<i>req-uri</i>	URI of HTTP request.	
	<i>resp-body</i>	HTTP response body.	
	<i>resp-hdr</i>	HTTP response headers.	
	<i>resp-status</i>	HTTP response status.	

config main-class

Parameter	Description	Type	Size
action	Action.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>allow</i>	Allow.	
	<i>block</i>	Block.	
	<i>erase</i>	Erase credit card numbers.	
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
severity	Severity.	option	-
	Option	Description	
	<i>high</i>	High severity.	
	<i>medium</i>	Medium severity.	
	<i>low</i>	Low severity.	
status	Status.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config url-access

Parameter	Description	Type	Size
action	Action.	option	-
	Option	Description	
	<i>bypass</i>	Allow the HTTP request, also bypass further WAF scanning.	
	<i>permit</i>	Allow the HTTP request, and continue further WAF scanning.	
	<i>block</i>	Block HTTP request.	

Parameter	Description	Type	Size
address	Host address.	string	Maximum length: 79
id	URL access ID.	integer	Minimum value: 0 Maximum value: 4294967295
log	Enable/disable logging.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

severity	Severity.	option	-

Option	Description
<i>high</i>	High severity.
<i>medium</i>	Medium severity.
<i>low</i>	Low severity.

config access-pattern

Parameter	Description	Type	Size
id	URL access pattern ID.	integer	Minimum value: 0 Maximum value: 4294967295
negate	Enable/disable match negation.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

pattern	URL pattern.	string	Maximum length: 511
regex	Enable/disable regular expression based pattern match.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
srcaddr	Source address.	string	Maximum length: 79

config waf signature

Hidden table for datasource.

```
config waf signature
    Description: Hidden table for datasource.
    edit <id>
        set desc {string}
    next
end
```

config waf signature

Parameter	Description	Type	Size
desc	Signature description.	string	Maximum length: 511
id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295

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
id	Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Signature subclass name.	string	Maximum length: 127

wanopt

This section includes syntax for the following commands:

- [config wanopt auth-group on page 1481](#)
- [config wanopt cache-service on page 1483](#)
- [config wanopt content-delivery-network-rule on page 1486](#)
- [config wanopt peer on page 1492](#)
- [config wanopt profile on page 1493](#)
- [config wanopt remote-storage on page 1503](#)
- [config wanopt settings on page 1504](#)
- [config wanopt webcache on page 1506](#)

config wanopt auth-group



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization authentication groups.

```
config wanopt auth-group
```

Description: Configure WAN optimization authentication groups.

```

edit <name>
    set auth-method [cert|psk]
    set cert {string}
    set peer {string}
    set peer-accept [any|defined|...]
    set psk {password}
next
end

```

config wanopt auth-group

Parameter	Description	Type	Size
auth-method	Select certificate or pre-shared key authentication for this authentication group.	option	-
	Option	Description	
	<i>cert</i>	Certificate authentication.	
	<i>psk</i>	Pre-shared secret key authentication.	
cert	Name of certificate to identify this peer.	string	Maximum length: 35
name	Auth-group name.	string	Maximum length: 35
peer	If peer-accept is set to one, select the name of one peer to add to this authentication group. The peer must have added with the wanopt peer command.	string	Maximum length: 35
peer-accept	Determine if this auth group accepts, any peer, a list of defined peers, or just one peer.	option	-
	Option	Description	
	<i>any</i>	Accept any peer that can authenticate with this auth group.	
	<i>defined</i>	Accept only the peers added with the wanopt peer command.	
	<i>one</i>	Accept the peer added to this auth group using the peer option.	
psk	Pre-shared key used by the peers in this authentication group.	password	Not Specified

config wanopt cache-service



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Designate cache-service for wan-optimization and webcache.

```
config wanopt cache-service
  Description: Designate cache-service for wan-optimization and webcache.
  set acceptable-connections [any|peers]
  set collaboration [enable|disable]
  set device-id {string}
  config dst-peer
    Description: Modify cache-service destination peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set ip {ipv4-address-any}
      set priority {integer}
    next
  end
  set prefer-scenario [balance|prefer-speed|...]
  config src-peer
    Description: Modify cache-service source peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set ip {ipv4-address-any}
      set priority {integer}
    next
  end
```

```
end
end
```

config wanopt cache-service

Parameter	Description	Type	Size
acceptable-connections	Set strategy when accepting cache collaboration connection.	option	-
		Option	Description
		<i>any</i>	We can accept any cache-collaboration connection.
		<i>peers</i>	We can only accept connections that are already in src-peers.
collaboration	Enable/disable cache-collaboration between cache-service clusters.	option	-
		Option	Description
		<i>enable</i>	Enable cache cache-collaboration.
		<i>disable</i>	Disable cache cache-collaboration.
device-id	Set identifier for this cache device.	string	Maximum length: 35
prefer-scenario	Set the preferred cache behavior towards the balance between latency and hit-ratio.	option	-
		Option	Description
		<i>balance</i>	Balance between speed and cache hit ratio.
		<i>prefer-speed</i>	Prefer response speed at the expense of increased cache bypasses.
		<i>prefer-cache</i>	Prefer improving hit-ratio through increasing latency tolerance.

config dst-peer

Parameter	Description	Type	Size
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255
device-id	Device ID of this peer.	string	Maximum length: 35

Parameter	Description	Type	Size
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255

config src-peer

Parameter	Description	Type	Size
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255
device-id	Device ID of this peer.	string	Maximum length: 35
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255

config wanopt content-delivery-network-rule



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization content delivery network rules.

```
config wanopt content-delivery-network-rule
  Description: Configure WAN optimization content delivery network rules.
  edit <name>
    set category [vcache|youtube]
    set comment {var-string}
    set host-domain-name-suffix <name1>, <name2>, ...
    set request-cache-control [enable|disable]
    set response-cache-control [enable|disable]
    set response-expires [enable|disable]
    config rules
      Description: WAN optimization content delivery network rule entries.
      edit <name>
        config content-id
          Description: Content ID settings.
          set end-direction [forward|backward]
          set end-skip {integer}
          set end-str {string}
          set range-str {string}
          set start-direction [forward|backward]
          set start-skip {integer}
          set start-str {string}
          set target [path|parameter|...]
        end
      end
    end
  end
```

```

    config match-entries
        Description: List of entries to match.
        edit <id>
            set pattern <string1>, <string2>, ...
            set target [path|parameter|...]
        next
    end
    set match-mode [all|any]
    config skip-entries
        Description: List of entries to skip.
        edit <id>
            set pattern <string1>, <string2>, ...
            set target [path|parameter|...]
        next
    end
    set skip-rule-mode [all|any]
next
end
set status [enable|disable]
set updateserver [enable|disable]
next
end

```

config wanopt content-delivery-network-rule

Parameter	Description	Type	Size
category	Content delivery network rule category.	option	-
	Option	Description	
	<i>vcache</i>	Vcache content delivery network.	
	<i>youtube</i>	Youtube content delivery network.	
comment	Comment about this CDN-rule.	var-string	Maximum length: 255
host-domain-name-suffix <name>	Suffix portion of the fully qualified domain name (eg. fortinet.com in "www.fortinet.com"). Suffix portion of the fully qualified domain name.	string	Maximum length: 79
name	Name of table.	string	Maximum length: 35
request-cache-control	Enable/disable HTTP request cache control.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size						
response-cache-control	Enable/disable HTTP response cache control.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
response-expires	Enable/disable HTTP response cache expires.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
status	Enable/disable WAN optimization content delivery network rules.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
updateserver	Enable/disable update server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

config rules

Parameter	Description	Type	Size
match-mode	Match criteria for collecting content ID.	option	-
	Option	Description	
	all	Must match all of the match entries.	
	any	Must match any of the match entries.	
name	WAN optimization content delivery network rule name.	string	Maximum length: 35
skip-rule-mode	Skip mode when evaluating skip-rules.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>all</i>	Must match all skip entries.	
	<i>any</i>	Must match any skip entries.	

config content-id

Parameter	Description	Type	Size
end-direction	Search direction from end-str match.	option	-
	Option	Description	
	<i>forward</i>	Forward direction.	
	<i>backward</i>	Backward direction.	
end-skip	Number of characters in URL to skip after end-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295
end-str	String from which to end search.	string	Maximum length: 35
range-str	Name of content ID within the start string and end string.	string	Maximum length: 35
start-direction	Search direction from start-str match.	option	-
	Option	Description	
	<i>forward</i>	Forward direction.	
	<i>backward</i>	Backward direction.	
start-skip	Number of characters in URL to skip after start-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295
start-str	String from which to start search.	string	Maximum length: 35
target	Option in HTTP header or URL parameter to match.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>path</i>	Match with the URL path.	
	<i>parameter</i>	Match with the URL parameters.	
	<i>referrer</i>	Match with the Referrer option in HTTP header.	
	<i>youtube-map</i>	Match Youtube content-id collection.	
	<i>youtube-id</i>	Match Youtube content-id.	
	<i>youku-id</i>	Match Youku content-id.	
	<i>hls-manifest</i>	Match with HLS manifest.	
	<i>dash-manifest</i>	Match with DASH manifest.	
	<i>hls-fragment</i>	Match HLS stream fragment.	
	<i>dash-fragment</i>	Match DASH stream fragment.	

config match-entries

Parameter	Description	Type	Size
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
pattern <string>	Pattern string for matching target (Referrer or URL pattern, eg. "a", "a*c", "**a*", "a*c*e", and "**"). Pattern strings.	string	Maximum length: 79
target	Option in HTTP header or URL parameter to match.	option	-

	Option	Description	
	<i>path</i>	Match with the URL path.	
	<i>parameter</i>	Match with the URL parameters.	
	<i>referrer</i>	Match with the Referrer option in HTTP header.	
	<i>youtube-map</i>	Match Youtube content-id collection.	
	<i>youtube-id</i>	Match Youtube content-id.	
	<i>youku-id</i>	Match Youku content-id.	

config skip-entries

Parameter	Description	Type	Size
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
pattern <string>	Pattern string for matching target (Referrer or URL pattern, eg. "a", "a*c", "**a*", "a*c*e", and "*"). Pattern strings.	string	Maximum length: 79
target	Option in HTTP header or URL parameter to match.	option	-

Option	Description
<i>path</i>	Match with the URL path.
<i>parameter</i>	Match with the URL parameters.
<i>referrer</i>	Match with the Referrer option in HTTP header.
<i>youtube-map</i>	Match Youtube content-id collection.
<i>youtube-id</i>	Match Youtube content-id.
<i>youku-id</i>	Match Youku content-id.

config wanopt peer



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization peers.

```
config wanopt peer
    Description: Configure WAN optimization peers.
    edit <peer-host-id>
        set ip {ipv4-address-any}
    next
end
```

config wanopt peer

Parameter	Description	Type	Size
ip	Peer IP address.	ipv4-address-any	Not Specified
peer-host-id	Peer host ID.	string	Maximum length: 35

config wanopt profile



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization profiles.

```
config wanopt profile
  Description: Configure WAN optimization profiles.
  edit <name>
    set auth-group {string}
    config cifs
      Description: Enable/disable CIFS (Windows sharing) WAN Optimization and
configure CIFS WAN Optimization features.
      set byte-caching [enable|disable]
      set log-traffic [enable|disable]
      set port {integer}
      set prefer-chunking [dynamic|fix]
      set secure-tunnel [enable|disable]
      set status [enable|disable]
      set tunnel-sharing [private|shared|...]
    end
    set comments {var-string}
    config ftp
      Description: Enable/disable FTP WAN Optimization and configure FTP WAN
Optimization features.
      set byte-caching [enable|disable]
      set log-traffic [enable|disable]
      set port {integer}
      set prefer-chunking [dynamic|fix]
```

```

        set secure-tunnel [enable|disable]
        set status [enable|disable]
        set tunnel-sharing [private|shared|...]
    end
    config http
        Description: Enable/disable HTTP WAN Optimization and configure HTTP WAN
        Optimization features.
        set byte-caching [enable|disable]
        set log-traffic [enable|disable]
        set port {integer}
        set prefer-chunking [dynamic|fix]
        set secure-tunnel [enable|disable]
        set ssl [enable|disable]
        set ssl-port {integer}
        set status [enable|disable]
        set tunnel-non-http [enable|disable]
        set tunnel-sharing [private|shared|...]
        set unknown-http-version [reject|tunnel|...]
    end
    config mapi
        Description: Enable/disable MAPI email WAN Optimization and configure MAPI WAN
        Optimization features.
        set byte-caching [enable|disable]
        set log-traffic [enable|disable]
        set port {integer}
        set secure-tunnel [enable|disable]
        set status [enable|disable]
        set tunnel-sharing [private|shared|...]
    end
    config tcp
        Description: Enable/disable TCP WAN Optimization and configure TCP WAN
        Optimization features.
        set byte-caching [enable|disable]
        set byte-caching-opt [mem-only|mem-disk]
        set log-traffic [enable|disable]
        set port {user}
        set secure-tunnel [enable|disable]
        set ssl [enable|disable]
        set ssl-port {integer}
        set status [enable|disable]
        set tunnel-sharing [private|shared|...]
    end
    set transparent [enable|disable]
next
end

```

config wanopt profile

Parameter	Description	Type	Size
auth-group	Optionally add an authentication group to restrict access to the WAN Optimization tunnel to peers in the authentication group.	string	Maximum length: 35

Parameter	Description	Type	Size
comments	Comment.	var-string	Maximum length: 255
name	Profile name.	string	Maximum length: 35
transparent	Enable/disable transparent mode.	option	-

Option	Description
<i>enable</i>	Determine if WAN Optimization changes client packet source addresses. Affects the routing configuration on the server network.
<i>disable</i>	Disable transparent mode. Client packets source addresses are changed to the source address of the FortiGate internal interface. Similar to source NAT.

config cifs

Parameter	Description	Type	Size
byte-caching	Enable/disable byte-caching for HTTP. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-

Option	Description
<i>enable</i>	Enable HTTP byte-caching.
<i>disable</i>	Disable HTTP byte-caching.

log-traffic	Enable/disable logging.	option	-

Option	Description
<i>enable</i>	Enable logging.
<i>disable</i>	Disable logging.

port	Single port number or port number range for CIFS. Only packets with a destination port number that matches this port number or range are accepted by this profile.	integer	Minimum value: 1 Maximum value: 65535

prefer-chunking	Select dynamic or fixed-size data chunking for HTTP WAN Optimization.	option	-

Option	Description
<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.
<i>fix</i>	Select fixed data chunking.

Parameter	Description	Type	Size								
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.				
Option	Description										
<i>enable</i>	Enable SSL-secured tunnelling.										
<i>disable</i>	Disable SSL-secured tunnelling.										
status	Enable/disable HTTP WAN Optimization.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP WAN Optimization.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP WAN Optimization.	<i>disable</i>	Disable HTTP WAN Optimization.				
Option	Description										
<i>enable</i>	Enable HTTP WAN Optimization.										
<i>disable</i>	Disable HTTP WAN Optimization.										
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr></table>	Option	Description	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
Option	Description										
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.										
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.										
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.										

config ftp

Parameter	Description	Type	Size						
byte-caching	Enable/disable byte-caching for HTTP. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP byte-caching.	<i>disable</i>	Disable HTTP byte-caching.		
Option	Description								
<i>enable</i>	Enable HTTP byte-caching.								
<i>disable</i>	Disable HTTP byte-caching.								
log-traffic	Enable/disable logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.		
Option	Description								
<i>enable</i>	Enable logging.								
<i>disable</i>	Disable logging.								

Parameter	Description	Type	Size
port	Single port number or port number range for FTP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	integer	Minimum value: 1 Maximum value: 65535
prefer-chunking	Select dynamic or fixed-size data chunking for HTTP WAN Optimization.	option	-

Option	Description
<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.
<i>fix</i>	Select fixed data chunking.

secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-

Option	Description
<i>enable</i>	Enable SSL-secured tunnelling.
<i>disable</i>	Disable SSL-secured tunnelling.

status	Enable/disable HTTP WAN Optimization.	option	-

Option	Description
<i>enable</i>	Enable HTTP WAN Optimization.
<i>disable</i>	Disable HTTP WAN Optimization.

tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-

Option	Description
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.

config http

Parameter	Description	Type	Size						
byte-caching	Enable/disable byte-caching for HTTP. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP byte-caching.	<i>disable</i>	Disable HTTP byte-caching.		
Option	Description								
<i>enable</i>	Enable HTTP byte-caching.								
<i>disable</i>	Disable HTTP byte-caching.								
log-traffic	Enable/disable logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.		
Option	Description								
<i>enable</i>	Enable logging.								
<i>disable</i>	Disable logging.								
port	Single port number or port number range for HTTP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	integer	Minimum value: 1 Maximum value: 65535						
prefer-chunking	Select dynamic or fixed-size data chunking for HTTP WAN Optimization.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dynamic</i></td><td>Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.</td></tr><tr><td><i>fix</i></td><td>Select fixed data chunking.</td></tr></table>	Option	Description	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.	<i>fix</i>	Select fixed data chunking.		
Option	Description								
<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.								
<i>fix</i>	Select fixed data chunking.								
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.		
Option	Description								
<i>enable</i>	Enable SSL-secured tunnelling.								
<i>disable</i>	Disable SSL-secured tunnelling.								
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for HTTPS traffic in this tunnel.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL/TLS offloading.</td></tr><tr><td><i>disable</i></td><td>Disable SSL/TLS offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL/TLS offloading.	<i>disable</i>	Disable SSL/TLS offloading.		
Option	Description								
<i>enable</i>	Enable SSL/TLS offloading.								
<i>disable</i>	Disable SSL/TLS offloading.								

Parameter	Description	Type	Size								
ssl-port	Port on which to expect HTTPS traffic for SSL/TLS offloading.	integer	Minimum value: 1 Maximum value: 65535								
status	Enable/disable HTTP WAN Optimization.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP WAN Optimization.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP WAN Optimization.	<i>disable</i>	Disable HTTP WAN Optimization.				
Option	Description										
<i>enable</i>	Enable HTTP WAN Optimization.										
<i>disable</i>	Disable HTTP WAN Optimization.										
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td></tr><tr><td><i>disable</i></td><td>Drop or tear down non-HTTP sessions accepted by the profile.</td></tr></table>	Option	Description	<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.				
Option	Description										
<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.										
<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.										
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr></table>	Option	Description	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
Option	Description										
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.										
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.										
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.										
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td></tr><tr><td><i>tunnel</i></td><td>Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td></tr><tr><td><i>best-effort</i></td><td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td></tr></table>	Option	Description	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.		
Option	Description										
<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.										
<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.										
<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.										

config mapi

Parameter	Description	Type	Size								
byte-caching	Enable/disable byte-caching for HTTP. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP byte-caching.	<i>disable</i>	Disable HTTP byte-caching.				
Option	Description										
<i>enable</i>	Enable HTTP byte-caching.										
<i>disable</i>	Disable HTTP byte-caching.										
log-traffic	Enable/disable logging.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.				
Option	Description										
<i>enable</i>	Enable logging.										
<i>disable</i>	Disable logging.										
port	Single port number or port number range for MAPI. Only packets with a destination port number that matches this port number or range are accepted by this profile.	integer	Minimum value: 1 Maximum value: 65535								
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.				
Option	Description										
<i>enable</i>	Enable SSL-secured tunnelling.										
<i>disable</i>	Disable SSL-secured tunnelling.										
status	Enable/disable HTTP WAN Optimization.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP WAN Optimization.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP WAN Optimization.	<i>disable</i>	Disable HTTP WAN Optimization.				
Option	Description										
<i>enable</i>	Enable HTTP WAN Optimization.										
<i>disable</i>	Disable HTTP WAN Optimization.										
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr></table>	Option	Description	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
Option	Description										
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.										
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.										
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.										

config tcp

Parameter	Description	Type	Size						
byte-caching	Enable/disable byte-caching for HTTP. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP byte-caching.	<i>disable</i>	Disable HTTP byte-caching.		
Option	Description								
<i>enable</i>	Enable HTTP byte-caching.								
<i>disable</i>	Disable HTTP byte-caching.								
byte-caching-opt	Select whether TCP byte-caching uses system memory only or both memory and disk space.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mem-only</i></td><td>Byte caching with memory only.</td></tr><tr><td><i>mem-disk</i></td><td>Byte caching with memory and disk.</td></tr></table>	Option	Description	<i>mem-only</i>	Byte caching with memory only.	<i>mem-disk</i>	Byte caching with memory and disk.		
Option	Description								
<i>mem-only</i>	Byte caching with memory only.								
<i>mem-disk</i>	Byte caching with memory and disk.								
log-traffic	Enable/disable logging.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.		
Option	Description								
<i>enable</i>	Enable logging.								
<i>disable</i>	Disable logging.								
port	Single port number or port number range for TCP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	user	Not Specified						
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.		
Option	Description								
<i>enable</i>	Enable SSL-secured tunnelling.								
<i>disable</i>	Disable SSL-secured tunnelling.								
ssl	Enable/disable SSL/TLS offloading.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL/TLS offloading.</td></tr><tr><td><i>disable</i></td><td>Disable SSL/TLS offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL/TLS offloading.	<i>disable</i>	Disable SSL/TLS offloading.		
Option	Description								
<i>enable</i>	Enable SSL/TLS offloading.								
<i>disable</i>	Disable SSL/TLS offloading.								

Parameter	Description	Type	Size
ssl-port	Port on which to expect HTTPS traffic for SSL/TLS offloading.	integer	Minimum value: 1 Maximum value: 65535
status	Enable/disable HTTP WAN Optimization.	option	-

Option	Description
<i>enable</i>	Enable HTTP WAN Optimization.
<i>disable</i>	Disable HTTP WAN Optimization.

tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-

Option	Description
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.

config wanopt remote-storage



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure a remote cache device as Web cache storage.

```
config wanopt remote-storage
    Description: Configure a remote cache device as Web cache storage.
    set local-cache-id {string}
    set remote-cache-id {string}
    set remote-cache-ip {ipv4-address-any}
    set status [disable|enable]
end
```

config wanopt remote-storage

Parameter	Description	Type	Size
local-cache-id	ID that this device uses to connect to the remote device.	string	Maximum length: 35
remote-cache-id	ID of the remote device to which the device connects.	string	Maximum length: 35
remote-cache-ip	IP address of the remote device to which the device connects.	ipv4-address-any	Not Specified

Parameter	Description	Type	Size
status	Enable/disable using remote device as Web cache storage.	option	-

Option	Description
<i>disable</i>	Use local disks as Web cache storage.
<i>enable</i>	Use a remote device as Web cache storage.

config wanopt settings



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization settings.

```
config wanopt settings
    Description: Configure WAN optimization settings.
    set auto-detect-algorithm [simple|diff-req-resp]
    set host-id {string}
    set tunnel-ssl-algorithm [high|medium|...]
end
```


config wanopt settings

Parameter	Description	Type	Size
auto-detect-algorithm	Auto detection algorithms used in tunnel negotiations.	option	-
	Option	Description	
	<i>simple</i>	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.	
	<i>diff-req-resp</i>	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.	
host-id	Local host ID (must also be entered in the remote FortiGate's peer list).	string	Maximum length: 35
tunnel-ssl-algorithm	Relative strength of encryption algorithms accepted during tunnel negotiation.	option	-
	Option	Description	
	<i>high</i>	High encryption. Allow only AES and ChaCha.	
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	

config wanopt webcache



This command is available for model(s): FortiGate 1000D, FortiGate 100D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 140D-POE, FortiGate 140D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 201E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300D, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3810D, FortiGate 3815D, FortiGate 401E, FortiGate 5001D, FortiGate 5001E1, FortiGate 500D, FortiGate 501E, FortiGate 51E, FortiGate 52E, FortiGate 600D, FortiGate 601E, FortiGate 61E, FortiGate 61F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate 92D, FortiGate-VM64, FortiWiFi 51E, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 2200E, FortiGate 300E, FortiGate 30E 3G4G GBL, FortiGate 30E 3G4G INTL, FortiGate 30E 3G4G NAM, FortiGate 30E, FortiGate 3300E, FortiGate 3400E, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400D, FortiGate 400E Bypass, FortiGate 400E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E, FortiGate 500E, FortiGate 50E, FortiGate 600E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 30D, FortiGateRugged 35D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiGateRugged 90D, FortiWiFi 30E 3G4G INTL, FortiWiFi 30E 3G4G NAM, FortiWiFi 30E, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 50E 2R, FortiWiFi 50E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure global Web cache settings.

```
config wanopt webcache
    Description: Configure global Web cache settings.
    set always-revalidate [enable|disable]
    set cache-by-default [enable|disable]
    set cache-cookie [enable|disable]
    set cache-expired [enable|disable]
    set default-ttl {integer}
    set external [enable|disable]
    set fresh-factor {integer}
    set host-validate [enable|disable]
    set ignore-conditional [enable|disable]
    set ignore-ie-reload [enable|disable]
    set ignore-ims [enable|disable]
    set ignore-pnc [enable|disable]
    set max-object-size {integer}
    set max-ttl {integer}
    set min-ttl {integer}
    set neg-resp-time {integer}
    set reval-pnc [enable|disable]
end
```

config wanopt webcache

Parameter	Description	Type	Size						
always-revalidate	Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable revalidation of requested cached objects.</td></tr><tr><td><i>disable</i></td><td>Disable revalidation of requested cached objects.</td></tr></table>	Option	Description	<i>enable</i>	Enable revalidation of requested cached objects.	<i>disable</i>	Disable revalidation of requested cached objects.		
Option	Description								
<i>enable</i>	Enable revalidation of requested cached objects.								
<i>disable</i>	Disable revalidation of requested cached objects.								
cache-by-default	Enable/disable caching content that lacks explicit caching policies from the server.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable caching content that lacks explicit caching policies.</td></tr><tr><td><i>disable</i></td><td>Disable caching content that lacks explicit caching policies.</td></tr></table>	Option	Description	<i>enable</i>	Enable caching content that lacks explicit caching policies.	<i>disable</i>	Disable caching content that lacks explicit caching policies.		
Option	Description								
<i>enable</i>	Enable caching content that lacks explicit caching policies.								
<i>disable</i>	Disable caching content that lacks explicit caching policies.								
cache-cookie	Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Cache cookies.</td></tr><tr><td><i>disable</i></td><td>Do not cache cookies.</td></tr></table>	Option	Description	<i>enable</i>	Cache cookies.	<i>disable</i>	Do not cache cookies.		
Option	Description								
<i>enable</i>	Cache cookies.								
<i>disable</i>	Do not cache cookies.								
cache-expired	Enable/disable caching type-1 objects that are already expired on arrival.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
default-ttl	Default object expiry time (default = 1440 min (1 day); maximum = 5256000 min (10 years)). This only applies to those objects that do not have an expiry time set by the web server.	integer	Minimum value: 1 Maximum value: 5256000						
external	Enable/disable external Web caching.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable external Web caching.</td></tr><tr><td><i>disable</i></td><td>Disable external Web caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable external Web caching.	<i>disable</i>	Disable external Web caching.		
Option	Description								
<i>enable</i>	Enable external Web caching.								
<i>disable</i>	Disable external Web caching.								

Parameter	Description	Type	Size
fresh-factor	Frequency that the server is checked to see if any objects have expired (1 - 100, default = 100). The higher the fresh factor, the less often the checks occur.	integer	Minimum value: 1 Maximum value: 100
host-validate	Enable/disable validating "Host:" with original server IP.	option	-

Option	Description
<i>enable</i>	Enable validating "Host:" with original server IP.
<i>disable</i>	Disable validating "Host:" with original server IP.

ignore-conditional	Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.	option	-

Option	Description
<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.
<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.

ignore-ie-reload	Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	option	-

Option	Description
<i>enable</i>	Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.
<i>disable</i>	Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.

ignore-ims	Enable/disable ignoring the if-modified-since (IMS) header.	option	-

Option	Description
<i>enable</i>	Enable ignoring the if-modified-since (IMS) header.
<i>disable</i>	Disable ignoring the if-modified-since (IMS) header.

ignore-pnc	Enable/disable ignoring the pragma no-cache (PNC) header.	option	-

Option	Description
<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.
<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.

Parameter	Description	Type	Size
max-object-size	Maximum cacheable object size in kB (1 - 2147483 kb (2GB). All objects that exceed this are delivered to the client but not stored in the web cache.	integer	Minimum value: 1 Maximum value: 2147483
max-ttl	Maximum time an object can stay in the web cache without checking to see if it has expired on the server (default = 7200 min (5 days); maximum = 5256000 min (10 years)).	integer	Minimum value: 1 Maximum value: 5256000
min-ttl	Minimum time an object can stay in the web cache without checking to see if it has expired on the server (default = 5 min; maximum = 5256000 (10 years)).	integer	Minimum value: 1 Maximum value: 5256000
neg-resp-time	Time in minutes to cache negative responses or errors (0 - 4294967295, default = 0 which means negative responses are not cached).	integer	Minimum value: 0 Maximum value: 4294967295
reval-pnc	Enable/disable revalidation of pragma-no-cache (PNC) to address bandwidth concerns.	option	-

Option	Description
<i>enable</i>	Enable revalidation of pragma-no-cache (PNC).
<i>disable</i>	Disable revalidation of pragma-no-cache (PNC).

web-proxy

This section includes syntax for the following commands:

- [config web-proxy debug-url on page 1510](#)
- [config web-proxy explicit on page 1511](#)
- [config web-proxy forward-server-group on page 1517](#)
- [config web-proxy forward-server on page 1516](#)
- [config web-proxy global on page 1518](#)
- [config web-proxy profile on page 1521](#)
- [config web-proxy url-match on page 1525](#)
- [config web-proxy wisp on page 1526](#)

config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
  Description: Configure debug URL addresses.
  edit <name>
    set exact [enable|disable]
    set status [enable|disable]
    set url-pattern {string}
  next
end
```

config web-proxy debug-url

Parameter	Description	Type	Size
exact	Enable/disable matching the exact path.	option	-
	Option	Description	
	<i>enable</i>	Enable matching the exact path.	
	<i>disable</i>	Disable matching the exact path.	
name	Debug URL name.	string	Maximum length: 63
status	Enable/disable this URL exemption.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable this URL exemption.	
	<i>disable</i>	Disable this URL exemption.	
url-pattern	URL exemption pattern.	string	Maximum length: 511

config web-proxy explicit

Configure explicit Web proxy settings.

```
config web-proxy explicit
    Description: Configure explicit Web proxy settings.
    set ftp-incoming-port {user}
    set ftp-over-http [enable|disable]
    set http-incoming-port {user}
    set https-incoming-port {user}
    set https-replacement-message [enable|disable]
    set incoming-ip {ipv4-address-any}
    set incoming-ip6 {ipv6-address}
    set ipv6-status [enable|disable]
    set message-upon-server-error [enable|disable]
    set outgoing-ip {ipv4-address-any}
    set outgoing-ip6 {ipv6-address}
    set pac-file-data {user}
    set pac-file-name {string}
    set pac-file-server-port {user}
    set pac-file-server-status [enable|disable]
    set pac-file-url {user}
    config pac-policy
        Description: PAC policies.
        edit <policyid>
            set comments {var-string}
            set dstaddr <name1>, <name2>, ...
            set pac-file-data {user}
            set pac-file-name {string}
            set srcaddr <name1>, <name2>, ...
            set srcaddr6 <name1>, <name2>, ...
            set status [enable|disable]
        next
    end
    set pref-dns-result [ipv4|ipv6]
    set realm {string}
    set sec-default-action [accept|deny]
    set socks [enable|disable]
    set socks-incoming-port {user}
    set ssl-algorithm [high|medium|...]
    set status [enable|disable]
    set strict-guest [enable|disable]
    set trace-auth-no-rsp [enable|disable]
```

```

set unknown-http-version [reject|best-effort]
end

```

config web-proxy explicit

Parameter	Description	Type	Size						
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports (0 - 65535, default = 0; use the same as HTTP).	user	Not Specified						
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FTP-over-HTTP sessions.</td></tr><tr><td><i>disable</i></td><td>Disable FTP-over-HTTP sessions.</td></tr></table>	Option	Description	<i>enable</i>	Enable FTP-over-HTTP sessions.	<i>disable</i>	Disable FTP-over-HTTP sessions.		
Option	Description								
<i>enable</i>	Enable FTP-over-HTTP sessions.								
<i>disable</i>	Disable FTP-over-HTTP sessions.								
http-incoming-port	Accept incoming HTTP requests on one or more ports (0 - 65535, default = 8080).	user	Not Specified						
https-incoming-port	Accept incoming HTTPS requests on one or more ports (0 - 65535, default = 0, use the same as HTTP).	user	Not Specified						
https-replacement-message	Enable/disable sending the client a replacement message for HTTPS requests.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display a replacement message for HTTPS requests.</td></tr><tr><td><i>disable</i></td><td>Do not display a replacement message for HTTPS requests.</td></tr></table>	Option	Description	<i>enable</i>	Display a replacement message for HTTPS requests.	<i>disable</i>	Do not display a replacement message for HTTPS requests.		
Option	Description								
<i>enable</i>	Display a replacement message for HTTPS requests.								
<i>disable</i>	Do not display a replacement message for HTTPS requests.								
incoming-ip	Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified						
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						
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowing an IPv6 web proxy destination.</td></tr><tr><td><i>disable</i></td><td>Disable allowing an IPv6 web proxy destination.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowing an IPv6 web proxy destination.	<i>disable</i>	Disable allowing an IPv6 web proxy destination.		
Option	Description								
<i>enable</i>	Enable allowing an IPv6 web proxy destination.								
<i>disable</i>	Disable allowing an IPv6 web proxy destination.								

Parameter	Description	Type	Size						
message-upon-server-error	Enable/disable displaying a replacement message when a server error is detected.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display a replacement message when a server error is detected.</td></tr><tr><td><i>disable</i></td><td>Do not display a replacement message when a server error is detected.</td></tr></table>	Option	Description	<i>enable</i>	Display a replacement message when a server error is detected.	<i>disable</i>	Do not display a replacement message when a server error is detected.		
Option	Description								
<i>enable</i>	Display a replacement message when a server error is detected.								
<i>disable</i>	Do not display a replacement message when a server error is detected.								
outgoing-ip	Outgoing HTTP requests will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified						
outgoing-ip6	Outgoing HTTP requests will leave this IPv6. Multiple interfaces can be specified. Interfaces must have these IPv6 addresses.	ipv6-address	Not Specified						
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified						
pac-file-name	Pac file name.	string	Maximum length: 63						
pac-file-server-port	Port number that PAC traffic from client web browsers uses to connect to the explicit web proxy (0 - 65535, default = 0; use the same as HTTP).	user	Not Specified						
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Proxy Auto-Configuration (PAC).</td></tr><tr><td><i>disable</i></td><td>Disable Proxy Auto-Configuration (PAC).</td></tr></table>	Option	Description	<i>enable</i>	Enable Proxy Auto-Configuration (PAC).	<i>disable</i>	Disable Proxy Auto-Configuration (PAC).		
Option	Description								
<i>enable</i>	Enable Proxy Auto-Configuration (PAC).								
<i>disable</i>	Disable Proxy Auto-Configuration (PAC).								
pac-file-url	PAC file access URL. Read-only.	user	Not Specified						
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server (default = ipv4).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Prefer the IPv4 DNS server.</td></tr><tr><td><i>ipv6</i></td><td>Prefer the IPv6 DNS server.</td></tr></table>	Option	Description	<i>ipv4</i>	Prefer the IPv4 DNS server.	<i>ipv6</i>	Prefer the IPv6 DNS server.		
Option	Description								
<i>ipv4</i>	Prefer the IPv4 DNS server.								
<i>ipv6</i>	Prefer the IPv6 DNS server.								
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	-						

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.</td></tr><tr><td><i>deny</i></td><td>Deny requests unless there is a matching explicit web proxy policy.</td></tr></table>	Option	Description	<i>accept</i>	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.	<i>deny</i>	Deny requests unless there is a matching explicit web proxy policy.				
Option	Description										
<i>accept</i>	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.										
<i>deny</i>	Deny requests unless there is a matching explicit web proxy policy.										
socks	Enable/disable the SOCKS proxy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the SOCKS proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the SOCKS proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the SOCKS proxy.	<i>disable</i>	Disable the SOCKS proxy.				
Option	Description										
<i>enable</i>	Enable the SOCKS proxy.										
<i>disable</i>	Disable the SOCKS proxy.										
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports (0 - 65535, default = 0; use the same as HTTP).	user	Not Specified								
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High enrption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High enrption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
Option	Description										
<i>high</i>	High enrption. Allow only AES and ChaCha.										
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.										
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.										
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the explicit web proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit web proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the explicit web proxy.	<i>disable</i>	Disable the explicit web proxy.				
Option	Description										
<i>enable</i>	Enable the explicit web proxy.										
<i>disable</i>	Disable the explicit web proxy.										
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict guest user checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict guest user checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict guest user checking.	<i>disable</i>	Disable strict guest user checking.				
Option	Description										
<i>enable</i>	Enable strict guest user checking.										
<i>disable</i>	Disable strict guest user checking.										
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-								

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable logging timed-out authentication requests.	
	<i>disable</i>	Disable logging timed-out authentication requests.	
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	
	<i>reject</i>	Reject requests with an unknown HTTP version.	
	<i>best-effort</i>	Accept requests with an unknown HTTP version and use best efforts to handle the session.	

config pac-policy

Parameter	Description	Type	Size
comments	Optional comments.	var-string	Maximum length: 1023
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified
pac-file-name	Pac file name.	string	Maximum length: 63
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 100
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79
status	Enable/disable policy.	option	-
	Option	Description	
	<i>enable</i>	Enable policy.	
	<i>disable</i>	Disable policy.	

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 comment {string}
    set fqdn {string}
    set healthcheck [disable|enable]
    set ip {ipv4-address-any}
    set monitor {string}
    set port {integer}
    set server-down-option [block|pass]
  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
		<i>ip</i>	Use an IP address for the forwarding proxy server.
		<i>fqdn</i>	Use the FQDN for the forwarding proxy server.
comment	Comment.	string	Maximum length: 63
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-
		Option	Description
		<i>disable</i>	Disable health checking.
		<i>enable</i>	Enable health checking.
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified
monitor	URL for forward server health check monitoring (default = http://www.google.com).	string	Maximum length: 255

Parameter	Description	Type	Size
name	Server name.	string	Maximum length: 63
port	Port number that the forwarding server expects to receive HTTP sessions on (1 - 65535, default = 3128).	integer	Minimum value: 1 Maximum value: 65535
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
<i>block</i>	Block sessions until the server is back up.
<i>pass</i>	Pass sessions to their destination bypassing the forward server.

config web-proxy forward-server-group

Configure a forward server group consisting of multiple forward servers. Supports failover and load balancing.

```
config web-proxy forward-server-group
    Description: Configure a forward server group consisting of multiple forward servers.
    Supports failover and load balancing.
    edit <name>
        set affinity [enable|disable]
        set group-down-option [block|pass]
        set ldb-method [weighted|least-session|...]
        config server-list
            Description: Add web forward servers to a list to form a server group.
            Optionally assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end
```

config web-proxy forward-server-group

Parameter	Description	Type	Size
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	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable affinity.	
	<i>disable</i>	Disable affinity.	
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	
	<i>block</i>	Block sessions until at least one server in the group is back up.	
	<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.	
ldb-method	Load balance method: weighted or least-session.	option	-
	Option	Description	
	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.	
	<i>least-session</i>	Send new sessions to the server with lowest session count.	
	<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.	
name	Configure a forward server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63

config server-list

Parameter	Description	Type	Size
name	Forward server name.	string	Maximum length: 63
weight	Optionally assign a weight of the forwarding server for weighted load balancing (1 - 100, default = 10)	integer	Minimum value: 1 Maximum value: 100

config web-proxy global

Configure Web proxy global settings.

```

config web-proxy global
    Description: Configure Web proxy global settings.
    set fast-policy-match [enable|disable]
    set forward-proxy-auth [enable|disable]
    set forward-server-affinity-timeout {integer}
    set learn-client-ip [enable|disable]
    set learn-client-ip-from-header {option1}, {option2}, ...
    set learn-client-ip-srcaddr <name1>, <name2>, ...
    set learn-client-ip-srcaddr6 <name1>, <name2>, ...
    set max-message-length {integer}
    set max-request-length {integer}
    set max-waf-body-cache-length {integer}
    set proxy-fqdn {string}
    set ssl-ca-cert {string}
    set ssl-cert {string}
    set strict-web-check [enable|disable]
    set tunnel-non-http [enable|disable]
    set unknown-http-version [reject|tunnel|...]
    set webproxy-profile {string}
end

```

config web-proxy global

Parameter	Description	Type	Size						
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forwarding proxy authentication headers.</td></tr><tr><td><i>disable</i></td><td>Disable forwarding proxy authentication headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable forwarding proxy authentication headers.	<i>disable</i>	Disable forwarding proxy authentication headers.		
Option	Description								
<i>enable</i>	Enable forwarding proxy authentication headers.								
<i>disable</i>	Disable forwarding proxy authentication headers.								
forward-server-affinity-timeout	Period of time before the source IP's traffic is no longer assigned to the forwarding server (6 - 60 min, default = 30).	integer	Minimum value: 6 Maximum value: 60						
learn-client-ip	Enable/disable learning the client's IP address from headers.	option	-						

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable learning the client's IP address from headers.</td></tr><tr><td><i>disable</i></td><td>Disable learning the client's IP address from headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable learning the client's IP address from headers.	<i>disable</i>	Disable learning the client's IP address from headers.				
	Option	Description									
	<i>enable</i>	Enable learning the client's IP address from headers.									
<i>disable</i>	Disable learning the client's IP address from headers.										
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>true-client-ip</i></td><td>Learn the client IP address from the True-Client-IP header.</td></tr><tr><td><i>x-real-ip</i></td><td>Learn the client IP address from the X-Real-IP header.</td></tr><tr><td><i>x-forwarded-for</i></td><td>Learn the client IP address from the X-Forwarded-For header.</td></tr></table>	Option	Description	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.	<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.	<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.		
	Option	Description									
	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.									
	<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.									
<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.										
learn-client-ip-srcaddr <name>	Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79								
learn-client-ip-srcaddr6 <name>	IPv6 Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79								
max-message-length	Maximum length of HTTP message, not including body (16 - 256 Kbytes, default = 32).	integer	Minimum value: 16 Maximum value: 256								
max-request-length	Maximum length of HTTP request line (2 - 64 Kbytes, default = 8).	integer	Minimum value: 2 Maximum value: 64								
max-waf-body-cache-length	Maximum length of HTTP messages processed by Web Application Firewall (WAF) (10 - 1024 Kbytes, default = 32).	integer	Minimum value: 10 Maximum value: 1024								
proxy-fqdn	Fully Qualified Domain Name (FQDN) that clients connect to (default = default.fqdn) to connect to the explicit web proxy.	string	Maximum length: 255								
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35								
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35								
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	-								

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict web checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict web checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict web checking.	<i>disable</i>	Disable strict web checking.				
	Option	Description									
	<i>enable</i>	Enable strict web checking.									
<i>disable</i>	Disable strict web checking.										
tunnel-non-http	Enable/disable allowing non-HTTP traffic. Allowed non-HTTP traffic is tunneled.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow non-HTTP traffic.</td></tr><tr><td><i>disable</i></td><td>Block non-HTTP traffic.</td></tr></table>	Option	Description	<i>enable</i>	Allow non-HTTP traffic.	<i>disable</i>	Block non-HTTP traffic.				
	Option	Description									
	<i>enable</i>	Allow non-HTTP traffic.									
<i>disable</i>	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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Rejects requests with unknown HTTP version.</td></tr><tr><td><i>tunnel</i></td><td>Tunnels requests with unknown HTTP version.</td></tr><tr><td><i>best-effort</i></td><td>Allow unknown HTTP requests and process them using best efforts.</td></tr></table>	Option	Description	<i>reject</i>	Rejects requests with unknown HTTP version.	<i>tunnel</i>	Tunnels requests with unknown HTTP version.	<i>best-effort</i>	Allow unknown HTTP requests and process them using best efforts.		
	Option	Description									
	<i>reject</i>	Rejects requests with unknown HTTP version.									
	<i>tunnel</i>	Tunnels requests with unknown HTTP version.									
<i>best-effort</i>	Allow unknown HTTP requests and process them using best efforts.										
webproxy-profile	Name of the web proxy profile to apply when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.	string	Maximum length: 63								

config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
  Description: Configure web proxy profiles.
  edit <name>
    set header-client-ip [pass|add|...]
    set header-front-end-https [pass|add|...]
    set header-via-request [pass|add|...]
    set header-via-response [pass|add|...]
    set header-x-authenticated-groups [pass|add|...]
    set header-x-authenticated-user [pass|add|...]
    set header-x-forwarded-for [pass|add|...]
    config headers
      Description: Configure HTTP forwarded requests headers.
      edit <id>
        set action [add-to-request|add-to-response|...]
        set add-option [append|new-on-not-found|...]
        set base64-encoding [disable|enable]
        set content {string}
```

```

        set dstaddr <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set name {string}
        set protocol {option1}, {option2}, ...
    next
end
set log-header-change [enable|disable]
set strip-encoding [enable|disable]
next
end

```

config web-proxy profile

Parameter	Description	Type	Size
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	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
header-front-end-https	Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
header-x-authenticated-groups	Action to take on the HTTP x-authenticated-groups header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
header-x-authenticated-user	Action to take on the HTTP x-authenticated-user header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
header-x-forwarded-for	Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-
	Option	Description	
	<i>pass</i>	Forward the same HTTP header.	
	<i>add</i>	Add the HTTP header.	
	<i>remove</i>	Remove the HTTP header.	
log-header-change	Enable/disable logging HTTP header changes.	option	-
	Option	Description	
	<i>enable</i>	Enable Enable/disable logging HTTP header changes.	
	<i>disable</i>	Disable Enable/disable logging HTTP header changes.	

Parameter	Description	Type	Size
name	Profile name.	string	Maximum length: 63
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-
	Option	Description	
	<i>enable</i>	Enable stripping of unsupported encoding from the request header.	
	<i>disable</i>	Disable stripping of unsupported encoding from the request header.	

config headers

Parameter	Description	Type	Size
action	Action when the HTTP header is forwarded.	option	-
	Option	Description	
	<i>add-to-request</i>	Add the HTTP header to request.	
	<i>add-to-response</i>	Add the HTTP header to response.	
	<i>remove-from-request</i>	Remove the HTTP header from request.	
	<i>remove-from-response</i>	Remove the HTTP header from response.	
add-option	Configure options to append content to existing HTTP header or add new HTTP header.	option	-
	Option	Description	
	<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.	
	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.	
	<i>new</i>	Create new header regardless if existing HTTP header is found or not.	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-
	Option	Description	
	<i>disable</i>	Disable use of base64 encoding of HTTP content.	
	<i>enable</i>	Enable use of base64 encoding of HTTP content.	

Parameter	Description	Type	Size
content	HTTP header content.	string	Maximum length: 255
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79
dstaddr6 <name>	Destination address and address group names (IPv6). Address name.	string	Maximum length: 79
id	HTTP forwarded header id.	integer	Minimum value: 0 Maximum value: 4294967295
name	HTTP forwarded header name.	string	Maximum length: 79
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-

Option	Description
<i>https</i>	Perform add-option action on HTTPS.
<i>http</i>	Perform add-option action on HTTP.

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 cache-exemption [enable|disable]
        set comment {var-string}
        set forward-server {string}
        set status [enable|disable]
        set url-pattern {string}
    next
end

```

config web-proxy url-match

Parameter	Description	Type	Size
cache-exemption	Enable/disable exempting this URL pattern from caching.	option	-
	Option	Description	
	<i>enable</i>	Enable exempting this URL pattern from caching.	
	<i>disable</i>	Disable exempting this URL pattern from caching.	
comment	Comment.	var-string	Maximum length: 255
forward-server	Forward server name.	string	Maximum length: 63
name	Configure a name for the URL to be exempted.	string	Maximum length: 63
status	Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding and caching.	option	-
	Option	Description	
	<i>enable</i>	Enable exempting the matching URLs.	
	<i>disable</i>	Disable exempting the matching URLs.	
url-pattern	URL pattern to be exempted from web proxy forwarding and caching.	string	Maximum length: 511

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 max-connections {integer}
    set outgoing-ip {ipv4-address-any}
    set server-ip {ipv4-address-any}
    set server-port {integer}
    set timeout {integer}
  next
end
```

config web-proxy wisp

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
max-connections	Maximum number of web proxy WISP connections (4 - 4096, default = 64).	integer	Minimum value: 4 Maximum value: 4096
name	Server name.	string	Maximum length: 35
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 (1 - 65535, default = 15868).	integer	Minimum value: 1 Maximum value: 65535
timeout	Period of time before WISP requests time out (1 - 15 sec, default = 5).	integer	Minimum value: 1 Maximum value: 15

webfilter

This section includes syntax for the following commands:

- [config webfilter content-header on page 1530](#)
- [config webfilter content on page 1528](#)
- [config webfilter fortiguard on page 1531](#)
- [config webfilter ftgd-local-cat on page 1533](#)
- [config webfilter ftgd-local-rating on page 1534](#)
- [config webfilter ips-urlfilter-cache-setting on page 1535](#)
- [config webfilter ips-urlfilter-setting on page 1535](#)
- [config webfilter ips-urlfilter-setting6 on page 1536](#)
- [config webfilter override on page 1536](#)
- [config webfilter profile on page 1538](#)
- [config webfilter search-engine on page 1554](#)
- [config webfilter urlfilter on page 1555](#)

config webfilter content

Configure Web filter banned word table.

```
config webfilter content
  Description: Configure Web filter banned word table.
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure banned word entries.
      edit <name>
        set action [block|exempt]
        set lang [western|simch|...]
        set pattern-type [wildcard|regexp]
        set score {integer}
        set status [enable|disable]
      next
    end
    set name {string}
  next
end
```


config webfilter content

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

config entries

Parameter	Description	Type	Size
action	Block or exempt word when a match is found.	option	-
	Option	Description	
	block	Block matches.	
	exempt	Exempt matches.	
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.	
name	Banned word.	string	Maximum length: 127
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>wildcard</i>	Wildcard pattern.	
	<i>regex</i>	Perl regular expression.	
score	Score, to be applied every time the word appears on a web page (0 - 4294967295, default = 10).	integer	Minimum value: 0 Maximum value: 4294967295
status	Enable/disable banned word.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

config webfilter content-header

Configure content types used by Web filter.

```
config webfilter content-header
    Description: Configure content types used by Web filter.
    edit <id>
        set comment {var-string}
        config entries
            Description: Configure content types used by web filter.
            edit <pattern>
                set action [block|allow|...]
                set category {user}
            next
        end
        set name {string}
    next
end
```

config webfilter content-header

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

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Name of table.	string	Maximum length: 63

config entries

Parameter	Description	Type	Size
action	Action to take for this content type.	option	-
	Option	Description	
	<i>block</i>	Block content type.	
	<i>allow</i>	Allow content type.	
	<i>exempt</i>	Exempt content type.	
category	Categories that this content type applies to.	user	Not Specified
pattern	Content type (regular expression).	string	Maximum length: 31

config webfilter fortiguard

Configure FortiGuard Web Filter service.

```
config webfilter fortiguard
    Description: Configure FortiGuard Web Filter service.
    set cache-mem-percent {integer}
    set cache-mode [ttl|db-ver]
    set cache-prefix-match [enable|disable]
    set close-ports [enable|disable]
    set ovr-auth-https [enable|disable]
    set ovr-auth-port-http {integer}
    set ovr-auth-port-https {integer}
    set ovr-auth-port-https-flow {integer}
    set ovr-auth-port-warning {integer}
    set request-packet-size-limit {integer}
    set warn-auth-https [enable|disable]
end
```

config webfilter fortiguard

Parameter	Description	Type	Size
cache-mem-percent	Maximum percentage of available memory allocated to caching (1 - 15%).	integer	Minimum value: 1 Maximum value: 15
cache-mode	Cache entry expiration mode.	option	-
	Option	Description	
	<i>tll</i>	Expire cache items by time-to-live.	
	<i>db-ver</i>	Expire cache items when the server DB version changes.	
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication	integer	Minimum value: 0 Maximum value: 65535

Parameter	Description	Type	Size
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
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server (0 for default).	integer	Minimum value: 576 Maximum value: 10000
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

```

config webfilter ftgd-local-cat
    Description: Configure FortiGuard Web Filter local categories.
    edit <desc>
        set id {integer}
        set status [enable|disable]
    next
end

```

config webfilter ftgd-local-cat

Parameter	Description	Type	Size
desc	Local category description.	string	Maximum length: 79
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191
status	Enable/disable the local category.	option	-
		Option	Description
		<i>enable</i>	Enable the local category.
		<i>disable</i>	Disable the local category.

config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

```
config webfilter ftgd-local-rating
  Description: Configure local FortiGuard Web Filter local ratings.
  edit <url>
    set rating {user}
    set status [enable|disable]
  next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size
rating	Local rating.	user	Not Specified
status	Enable/disable local rating.	option	-
		Option	Description
		<i>enable</i>	Enable local rating.
		<i>disable</i>	Disable local rating.
url	URL to rate locally.	string	Maximum length: 511

config webfilter 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 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 (1 - 255) for this route.	integer	Minimum value: 1 Maximum value: 255
gateway	Gateway IP address for this route.	ipv4-address	Not Specified

Parameter	Description	Type	Size
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 (1 - 255) 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 override

Configure FortiGuard Web Filter administrative overrides.

```
config webfilter override
    Description: Configure FortiGuard Web Filter administrative overrides.
    edit <id>
        set expires {user}
        set initiator {string}
        set ip {ipv4-address}
        set ip6 {ipv6-address}
        set new-profile {string}
        set old-profile {string}
    end
```



```

    set scope [user|user-group|...]
    set status [enable|disable]
    set user {string}
    set user-group {string}
next
end

```

config webfilter override

Parameter	Description	Type	Size
expires	Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).	user	Not Specified
id	Override rule ID.	integer	Minimum value: 0 Maximum value: 4294967295
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64
ip	IPv4 address which the override applies.	ipv4-address	Not Specified
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 35
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 35
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-
	Option Description		
	<i>user</i> Override the specified user.		
	<i>user-group</i> Override the specified user group.		
	<i>ip</i> Override the specified IP address.		
	<i>ip6</i> Override the specified IPv6 address.		
status	Enable/disable override rule.	option	-
	Option Description		
	<i>enable</i> Enable override rule.		
	<i>disable</i> Disable override rule.		

Parameter	Description	Type	Size
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

config webfilter profile

Configure Web filter profiles.

```

config webfilter profile
  Description: Configure Web filter profiles.
  edit <name>
    set comment {var-string}
    set extended-log [enable|disable]
    config file-filter
      Description: File filter.
      config entries
        Description: File filter entries.
        edit <filter>
          set action [log|block]
          set comment {var-string}
          set direction [incoming|outgoing|...]
          set file-type <name1>, <name2>, ...
          set password-protected [yes|any]
          set protocol {option1}, {option2}, ...
        next
      end
      set log [enable|disable]
      set scan-archive-contents [enable|disable]
      set status [enable|disable]
    end
  config ftgd-wf
    Description: FortiGuard Web Filter settings.
    set exempt-quota {user}
    config filters
      Description: FortiGuard filters.
      edit <id>
        set action [block|authenticate|...]
        set auth-usr-grp <name1>, <name2>, ...
        set category {integer}
        set log [enable|disable]
        set override-replacemsg {string}
        set warn-duration {user}
        set warning-duration-type [session|timeout]
        set warning-prompt [per-domain|per-category]
      next
    end
    set max-quota-timeout {integer}
    set options {option1}, {option2}, ...
    set ovrd {user}
    config quota

```

```

        Description: FortiGuard traffic quota settings.
        edit <id>
            set category {user}
            set duration {user}
            set override-replacemsg {string}
            set type [time|traffic]
            set unit [B|KB|...]
            set value {integer}
        next
    end
    set rate-crl-urls [disable|enable]
    set rate-css-urls [disable|enable]
    set rate-image-urls [disable|enable]
    set rate-javascript-urls [disable|enable]
end
set https-replacemsg [enable|disable]
set log-all-url [enable|disable]
set options {option1}, {option2}, ...
config override
    Description: Web Filter override settings.
    set ovr-dur {user}
    set ovr-dur-mode [constant|ask]
    set ovr-scope [user|user-group|...]
    set ovr-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set profile-type [list|radius]
end
set ovr-perm {option1}, {option2}, ...
set post-action [normal|block]
set replacemsg-group {string}
config web
    Description: Web content filtering settings.
    set blacklist [enable|disable]
    set bword-table {integer}
    set bword-threshold {integer}
    set content-header-list {integer}
    set keyword-match <pattern1>, <pattern2>, ...
    set log-search [enable|disable]
    set safe-search {option1}, {option2}, ...
    set urlfilter-table {integer}
    set whitelist {option1}, {option2}, ...
    set youtube-restrict [none|strict|...]
end
set web-content-log [enable|disable]
set web-extended-all-action-log [enable|disable]
set web-filter-activex-log [enable|disable]
set web-filter-applet-log [enable|disable]
set web-filter-command-block-log [enable|disable]
set web-filter-cookie-log [enable|disable]
set web-filter-cookie-removal-log [enable|disable]
set web-filter-js-log [enable|disable]
set web-filter-jscript-log [enable|disable]
set web-filter-referer-log [enable|disable]
set web-filter-unknown-log [enable|disable]

```

```

set web-filter-vbs-log [enable|disable]
set web-ftgd-err-log [enable|disable]
set web-ftgd-quota-usage [enable|disable]
set web-invalid-domain-log [enable|disable]
set web-url-log [enable|disable]
set wisp [enable|disable]
set wisp-algorithm [primary-secondary|round-robin|...]
set wisp-servers <name1>, <name2>, ...
config youtube-channel-filter
    Description: YouTube channel filter.
    edit <id>
        set channel-id {string}
        set comment {var-string}
    next
end
set youtube-channel-status [disable|blacklist|...]
next
end

```

config webfilter profile

Parameter	Description	Type	Size
comment	Optional comments.	var-string	Maximum length: 255
extended-log	Enable/disable extended logging for web filtering.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
https-replacemsg	Enable replacement messages for HTTPS.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
log-all-url	Enable/disable logging all URLs visited.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
name	Profile name.	string	Maximum length: 35
options	Options.	option	-

Parameter	Description	Type	Size																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>activexfilter</i></td><td>ActiveX filter.</td></tr><tr><td><i>cookiefilter</i></td><td>Cookie filter.</td></tr><tr><td><i>javafilter</i></td><td>Java applet filter.</td></tr><tr><td><i>block-invalid-url</i></td><td>Block sessions contained an invalid domain name.</td></tr><tr><td><i>jscript</i></td><td>Javascript block.</td></tr><tr><td><i>js</i></td><td>JS block.</td></tr><tr><td><i>vbs</i></td><td>VB script block.</td></tr><tr><td><i>unknown</i></td><td>Unknown script block.</td></tr><tr><td><i>intrinsic</i></td><td>Intrinsic script block.</td></tr><tr><td><i>wf-referer</i></td><td>Referring block.</td></tr><tr><td><i>wf-cookie</i></td><td>Cookie block.</td></tr><tr><td><i>per-user-bwl</i></td><td>Per-user black/white list filter</td></tr></table>	Option	Description	<i>activexfilter</i>	ActiveX filter.	<i>cookiefilter</i>	Cookie filter.	<i>javafilter</i>	Java applet filter.	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.	<i>jscript</i>	Javascript block.	<i>js</i>	JS block.	<i>vbs</i>	VB script block.	<i>unknown</i>	Unknown script block.	<i>intrinsic</i>	Intrinsic script block.	<i>wf-referer</i>	Referring block.	<i>wf-cookie</i>	Cookie block.	<i>per-user-bwl</i>	Per-user black/white list filter		
	Option	Description																											
	<i>activexfilter</i>	ActiveX filter.																											
	<i>cookiefilter</i>	Cookie filter.																											
	<i>javafilter</i>	Java applet filter.																											
	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.																											
	<i>jscript</i>	Javascript block.																											
	<i>js</i>	JS block.																											
	<i>vbs</i>	VB script block.																											
	<i>unknown</i>	Unknown script block.																											
	<i>intrinsic</i>	Intrinsic script block.																											
	<i>wf-referer</i>	Referring block.																											
	<i>wf-cookie</i>	Cookie block.																											
<i>per-user-bwl</i>	Per-user black/white list filter																												
ovrd-perm	Permitted override types.	option	-																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bannedword-override</i></td><td>Banned word override.</td></tr><tr><td><i>urlfilter-override</i></td><td>URL filter override.</td></tr><tr><td><i>fortiguard-wf-override</i></td><td>FortiGuard Web Filter override.</td></tr><tr><td><i>contenttype-check-override</i></td><td>Content-type header override.</td></tr></table>	Option	Description	<i>bannedword-override</i>	Banned word override.	<i>urlfilter-override</i>	URL filter override.	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.	<i>contenttype-check-override</i>	Content-type header override.																		
	Option	Description																											
	<i>bannedword-override</i>	Banned word override.																											
	<i>urlfilter-override</i>	URL filter override.																											
	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.																											
<i>contenttype-check-override</i>	Content-type header override.																												
post-action	Action taken for HTTP POST traffic.	option	-																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal, POST requests are allowed.</td></tr><tr><td><i>block</i></td><td>POST requests are blocked.</td></tr></table>	Option	Description	<i>normal</i>	Normal, POST requests are allowed.	<i>block</i>	POST requests are blocked.																						
	Option	Description																											
	<i>normal</i>	Normal, POST requests are allowed.																											
<i>block</i>	POST requests are blocked.																												
replacemsg-group	Replacement message group.	string	Maximum length: 35																										
web-content-log	Enable/disable logging logging blocked web content.	option	-																										

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
web-filter-activex-log	Enable/disable logging ActiveX.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
web-filter-applet-log	Enable/disable logging Java applets.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	

Parameter	Description	Type	Size						
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
web-filter-js-log	Enable/disable logging Java scripts.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
web-filter-jscript-log	Enable/disable logging JScripts.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
web-filter-referer-log	Enable/disable logging referrers.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								

Parameter	Description	Type	Size
web-ftgd-err-log	Enable/disable logging rating errors.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

web-url-log	Enable/disable logging URL filtering.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

wisp	Enable/disable web proxy WISP.	option	-

Option	Description
<i>enable</i>	Enable web proxy WISP.
<i>disable</i>	Disable web proxy WISP.

wisp-algorithm	WISP server selection algorithm.	option	-

Option	Description
<i>primary-secondary</i>	Select the first healthy server in order.
<i>round-robin</i>	Select the next healthy server.
<i>auto-learning</i>	Select the lightest loading healthy server.

Parameter	Description	Type	Size
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79
youtube- channel-status	YouTube channel filter status.	option	-

Option	Description
<i>disable</i>	Disable YouTube channel filter.
<i>blacklist</i>	Block matches.
<i>whitelist</i>	Allow matches.

config file-filter

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

Option	Description
<i>enable</i>	Enable file filter logging.
<i>disable</i>	Disable file filter logging.

scan-archive- contents	Enable/disable file filter archive contents scan.	option	-

Option	Description
<i>enable</i>	Enable file filter archive contents scan.
<i>disable</i>	Disable file filter archive contents scan.

status	Enable/disable file filter.	option	-

Option	Description
<i>enable</i>	Enable file filter.
<i>disable</i>	Disable file filter.

config entries

Parameter	Description	Type	Size
action	Action taken for matched file.	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>log</i></td><td>Allow the content and write a log message.</td></tr><tr><td><i>block</i></td><td>Block the content and write a log message.</td></tr></table>	Option	Description	<i>log</i>	Allow the content and write a log message.	<i>block</i>	Block the content and write a log message.				
	Option	Description									
	<i>log</i>	Allow the content and write a log message.									
<i>block</i>	Block the content and write a log message.										
comment	Comment.	var-string	Maximum length: 255								
direction	Match files transmitted in the session's originating or reply direction.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>incoming</i></td><td>Match files transmitted in the session's originating direction.</td></tr><tr><td><i>outgoing</i></td><td>Match files transmitted in the session's reply direction.</td></tr><tr><td><i>any</i></td><td>Match files transmitted in the session's originating and reply direction.</td></tr></table>	Option	Description	<i>incoming</i>	Match files transmitted in the session's originating direction.	<i>outgoing</i>	Match files transmitted in the session's reply direction.	<i>any</i>	Match files transmitted in the session's originating and reply direction.		
	Option	Description									
	<i>incoming</i>	Match files transmitted in the session's originating direction.									
	<i>outgoing</i>	Match files transmitted in the session's reply direction.									
<i>any</i>	Match files transmitted in the session's originating and reply direction.										
file-type <name>	Select file type. File type name.	string	Maximum length: 39								
filter	Add a file filter.	string	Maximum length: 35								
password-protected	Match password-protected files.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yes</i></td><td>Match only password-protected files.</td></tr><tr><td><i>any</i></td><td>Match any file.</td></tr></table>	Option	Description	<i>yes</i>	Match only password-protected files.	<i>any</i>	Match any file.				
	Option	Description									
	<i>yes</i>	Match only password-protected files.									
<i>any</i>	Match any file.										
protocol	Protocols to apply with.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Enable/disable HTTP.</td></tr><tr><td><i>ftp</i></td><td>Enable/disable FTP.</td></tr></table>	Option	Description	<i>http</i>	Enable/disable HTTP.	<i>ftp</i>	Enable/disable FTP.				
	Option	Description									
	<i>http</i>	Enable/disable HTTP.									
<i>ftp</i>	Enable/disable FTP.										

config ftgd-wf

Parameter	Description	Type	Size
exempt-quota	Do not stop quota for these categories.	user	Not Specified

Parameter	Description	Type	Size
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400
options	Options for FortiGuard Web Filter.	option	-

Option	Description

<i>error-allow</i>	Allow web pages with a rating error to pass through.
<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.
<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.
<i>ftgd-disable</i>	Disable FortiGuard scanning.

ovrd	Allow web filter profile overrides.	user	Not Specified

rate-crl-urls	Enable/disable rating CRL by URL.	option	-

Option	Description

<i>disable</i>	Disable rating CRL by URL.
<i>enable</i>	Enable rating CRL by URL.

rate-css-urls	Enable/disable rating CSS by URL.	option	-

Option	Description

<i>disable</i>	Disable rating CSS by URL.
<i>enable</i>	Enable rating CSS by URL.

rate-image-urls	Enable/disable rating images by URL.	option	-

Option	Description

<i>disable</i>	Disable rating images by URL (blocked images are replaced with blanks).
<i>enable</i>	Enable rating images by URL (blocked images are replaced with blanks).

rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-

Option	Description

<i>disable</i>	Disable rating JavaScript by URL.
<i>enable</i>	Enable rating JavaScript by URL.

config filters

Parameter	Description	Type	Size
action	Action to take for matches.	option	-
	Option	Description	
	<i>block</i>	Block access.	
	<i>authenticate</i>	Authenticate user before allowing access.	
	<i>monitor</i>	Allow access while logging the action.	
	<i>warning</i>	Allow access after warning the user.	
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255
id	ID number.	integer	Minimum value: 0 Maximum value: 255
log	Enable/disable logging.	option	-
	Option	Description	
	<i>enable</i>	Enable setting.	
	<i>disable</i>	Disable setting.	
override- replacemsg	Override replacement message.	string	Maximum length: 28
warn-duration	Duration of warnings.	user	Not Specified
warning- duration-type	Re-display warning after closing browser or after a timeout.	option	-
	Option	Description	
	<i>session</i>	After session ends.	
	<i>timeout</i>	After timeout occurs.	
warning- prompt	Warning prompts in each category or each domain.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>per-domain</i>	Per-domain warnings.	
	<i>per-category</i>	Per-category warnings.	

config quota

Parameter	Description	Type	Size
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified
duration	Duration of quota.	user	Not Specified
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295
override-replacemsg	Override replacement message.	string	Maximum length: 28
type	Quota type.	option	-

	Option	Description	
	<i>time</i>	Use a time-based quota.	
	<i>traffic</i>	Use a traffic-based quota.	

unit	Traffic quota unit of measurement.	option	-

	Option	Description	
	<i>B</i>	Quota in bytes.	
	<i>KB</i>	Quota in kilobytes.	
	<i>MB</i>	Quota in megabytes.	
	<i>GB</i>	Quota in gigabytes.	

value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295

config override

Parameter	Description	Type	Size												
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow browser-based (cookie) override.</td></tr><tr><td><i>deny</i></td><td>Deny browser-based (cookie) override.</td></tr></table>	Option	Description	<i>allow</i>	Allow browser-based (cookie) override.	<i>deny</i>	Deny browser-based (cookie) override.								
Option	Description														
<i>allow</i>	Allow browser-based (cookie) override.														
<i>deny</i>	Deny browser-based (cookie) override.														
ovrd-dur	Override duration.	user	Not Specified												
ovrd-dur-mode	Override duration mode.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>constant</i></td><td>Constant mode.</td></tr><tr><td><i>ask</i></td><td>Prompt for duration when initiating an override.</td></tr></table>	Option	Description	<i>constant</i>	Constant mode.	<i>ask</i>	Prompt for duration when initiating an override.								
Option	Description														
<i>constant</i>	Constant mode.														
<i>ask</i>	Prompt for duration when initiating an override.														
ovrd-scope	Override scope.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Override for the user.</td></tr><tr><td><i>user-group</i></td><td>Override for the user's group.</td></tr><tr><td><i>ip</i></td><td>Override for the initiating IP.</td></tr><tr><td><i>browser</i></td><td>Create browser-based (cookie) override.</td></tr><tr><td><i>ask</i></td><td>Prompt for scope when initiating an override.</td></tr></table>	Option	Description	<i>user</i>	Override for the user.	<i>user-group</i>	Override for the user's group.	<i>ip</i>	Override for the initiating IP.	<i>browser</i>	Create browser-based (cookie) override.	<i>ask</i>	Prompt for scope when initiating an override.		
Option	Description														
<i>user</i>	Override for the user.														
<i>user-group</i>	Override for the user's group.														
<i>ip</i>	Override for the initiating IP.														
<i>browser</i>	Create browser-based (cookie) override.														
<i>ask</i>	Prompt for scope when initiating an override.														
ovrd-user-group <name>	User groups with permission to use the override. User group name.	string	Maximum length: 79												
profile <name>	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79												
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>User-Name</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Netmask</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.				
Option	Description														
<i>User-Name</i>	Use this attribute.														
<i>NAS-IP-Address</i>	Use this attribute.														
<i>Framed-IP-Address</i>	Use this attribute.														
<i>Framed-IP-Netmask</i>	Use this attribute.														

Parameter	Description	Type	Size																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>Filter-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-IP-Host</i></td><td>Use this attribute.</td></tr><tr><td><i>Reply-Message</i></td><td>Use this attribute.</td></tr><tr><td><i>Callback-Number</i></td><td>Use this attribute.</td></tr><tr><td><i>Callback-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-Route</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IPX-Network</i></td><td>Use this attribute.</td></tr><tr><td><i>Class</i></td><td>Use this attribute.</td></tr><tr><td><i>Called-Station-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Calling-Station-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-Identifier</i></td><td>Use this attribute.</td></tr><tr><td><i>Proxy-State</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Service</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Node</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-LAT-Group</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-AppleTalk-Zone</i></td><td>Use this attribute.</td></tr><tr><td><i>Acct-Session-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Acct-Multi-Session-Id</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.	<i>Callback-Number</i>	Use this attribute.	<i>Callback-Id</i>	Use this attribute.	<i>Framed-Route</i>	Use this attribute.	<i>Framed-IPX-Network</i>	Use this attribute.	<i>Class</i>	Use this attribute.	<i>Called-Station-Id</i>	Use this attribute.	<i>Calling-Station-Id</i>	Use this attribute.	<i>NAS-Identifier</i>	Use this attribute.	<i>Proxy-State</i>	Use this attribute.	<i>Login-LAT-Service</i>	Use this attribute.	<i>Login-LAT-Node</i>	Use this attribute.	<i>Login-LAT-Group</i>	Use this attribute.	<i>Framed-AppleTalk-Zone</i>	Use this attribute.	<i>Acct-Session-Id</i>	Use this attribute.	<i>Acct-Multi-Session-Id</i>	Use this attribute.		
	Option	Description																																							
	<i>Filter-Id</i>	Use this attribute.																																							
	<i>Login-IP-Host</i>	Use this attribute.																																							
	<i>Reply-Message</i>	Use this attribute.																																							
	<i>Callback-Number</i>	Use this attribute.																																							
	<i>Callback-Id</i>	Use this attribute.																																							
	<i>Framed-Route</i>	Use this attribute.																																							
	<i>Framed-IPX-Network</i>	Use this attribute.																																							
	<i>Class</i>	Use this attribute.																																							
	<i>Called-Station-Id</i>	Use this attribute.																																							
	<i>Calling-Station-Id</i>	Use this attribute.																																							
	<i>NAS-Identifier</i>	Use this attribute.																																							
	<i>Proxy-State</i>	Use this attribute.																																							
	<i>Login-LAT-Service</i>	Use this attribute.																																							
	<i>Login-LAT-Node</i>	Use this attribute.																																							
	<i>Login-LAT-Group</i>	Use this attribute.																																							
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.																																							
	<i>Acct-Session-Id</i>	Use this attribute.																																							
	<i>Acct-Multi-Session-Id</i>	Use this attribute.																																							
profile-type	Override profile type.	option	-																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>list</i></td><td>Profile chosen from list.</td></tr><tr><td><i>radius</i></td><td>Profile determined by RADIUS server.</td></tr></table>	Option	Description	<i>list</i>	Profile chosen from list.	<i>radius</i>	Profile determined by RADIUS server.																																		
	Option	Description																																							
	<i>list</i>	Profile chosen from list.																																							
<i>radius</i>	Profile determined by RADIUS server.																																								

config web

Parameter	Description	Type	Size						
blacklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blacklist.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295						
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647						
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295						
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79						
log-search	Enable/disable logging all search phrases.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>			Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description								
<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.								
safe-search	Safe search type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>url</i></td><td>Insert safe search string into URL.</td></tr><tr><td><i>header</i></td><td>Insert safe search header.</td></tr></table>			Option	Description	<i>url</i>	Insert safe search string into URL.	<i>header</i>	Insert safe search header.
Option	Description								
<i>url</i>	Insert safe search string into URL.								
<i>header</i>	Insert safe search header.								

Parameter	Description	Type	Size
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295
whitelist	FortiGuard whitelist settings.	option	-

Option	Description
<i>exempt-av</i>	Exempt antivirus.
<i>exempt-webcontent</i>	Exempt web content.
<i>exempt-activex-java-cookie</i>	Exempt ActiveX-JAVA-Cookie.
<i>exempt-dlp</i>	Exempt DLP.
<i>exempt-rangeblock</i>	Exempt RangeBlock.
<i>extended-log-others</i>	Support extended log.

youtube-restrict	YouTube EDU filter level.	option	-

Option	Description
<i>none</i>	Full access for YouTube.
<i>strict</i>	Strict access for YouTube.
<i>moderate</i>	Moderate access for YouTube.

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
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295

config webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
  Description: Configure web filter search engines.
  edit <name>
    set charset [utf-8|gb2312]
    set hostname {string}
    set query {string}
    set safesearch [disable|url|...]
    set safesearch-str {string}
    set url {string}
  next
end
```

config webfilter search-engine

Parameter	Description	Type	Size
charset	Search engine charset.	option	-
	Option	Description	
	<i>utf-8</i>	UTF-8 encoding.	
	<i>gb2312</i>	GB2312 encoding.	
hostname	Hostname (regular expression).	string	Maximum length: 127
name	Search engine name.	string	Maximum length: 35
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-
	Option	Description	
	<i>disable</i>	Site does not support safe search.	
	<i>url</i>	Safe search selected with a parameter in the URL.	
	<i>header</i>	Safe search selected by search header (i.e. youtube.edu).	
safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79
url	URL (regular expression).	string	Maximum length: 127

config webfilter urlfilter

Configure URL filter lists.

```
config webfilter urlfilter
  Description: Configure URL filter lists.
  edit <id>
    set comment {var-string}
    config entries
      Description: URL filter entries.
      edit <id>
        set action [exempt|block|...]
        set dns-address-family [ipv4|ipv6|...]
        set exempt {option1}, {option2}, ...
        set referrer-host {string}
        set status [enable|disable]
        set type [simple|regex|...]
        set url {string}
        set web-proxy-profile {string}
      next
    end
    set ip-addr-block [enable|disable]
    set name {string}
    set one-arm-ips-urlfilter [enable|disable]
  next
end
```

config webfilter urlfilter

Parameter	Description	Type	Size
comment	Optional comments.	var-string	Maximum length: 255
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-
		Option	Description
		<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.
		<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.
name	Name of URL filter list.	string	Maximum length: 63

Parameter	Description	Type	Size
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-
	Option	Description	
	<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.	
	<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.	

config entries

Parameter	Description	Type	Size
action	Action to take for URL filter matches.	option	-
	Option	Description	
	<i>exempt</i>	Exempt matches.	
	<i>block</i>	Block matches.	
	<i>allow</i>	Allow matches (no log).	
	<i>monitor</i>	Allow matches (with log).	
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-
	Option	Description	
	<i>ipv4</i>	Resolve IPv4 address from DNS server.	
	<i>ipv6</i>	Resolve IPv6 address from DNS server.	
	<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.	
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-
	Option	Description	
	<i>av</i>	AntiVirus scanning.	
	<i>web-content</i>	Web filter content matching.	
	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.	
	<i>dlp</i>	DLP scanning.	
	<i>fortiguard</i>	FortiGuard web filtering.	

Parameter	Description	Type	Size
	Option	Description	
	<i>range-block</i>	Range block feature.	
	<i>pass</i>	Pass single connection from all.	
	<i>all</i>	Exempt from all security profiles.	
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295
referrer-host	Referrer host name.	string	Maximum length: 255
status	Enable/disable this URL filter.	option	-
	Option	Description	
	<i>enable</i>	Enable this URL filter.	
	<i>disable</i>	Disable this URL filter.	
type	Filter type (simple, regex, or wildcard).	option	-
	Option	Description	
	<i>simple</i>	Simple URL string.	
	<i>regex</i>	Regular expression URL string.	
	<i>wildcard</i>	Wildcard URL string.	
url	URL to be filtered.	string	Maximum length: 511
web-proxy-profile	Web proxy profile.	string	Maximum length: 63

wireless-controller

This section includes syntax for the following commands:

- [config wireless-controller address on page 1559](#)
- [config wireless-controller addrgrp on page 1559](#)
- [config wireless-controller ap-status on page 1560](#)
- [config wireless-controller ble-profile on page 1561](#)
- [config wireless-controller bonjour-profile on page 1563](#)
- [config wireless-controller global on page 1564](#)
- [config wireless-controller hotspot20 anqp-3gpp-cellular on page 1567](#)
- [config wireless-controller hotspot20 anqp-ip-address-type on page 1568](#)
- [config wireless-controller hotspot20 anqp-nai-realm on page 1569](#)
- [config wireless-controller hotspot20 anqp-network-auth-type on page 1572](#)
- [config wireless-controller hotspot20 anqp-roaming-consortium on page 1573](#)
- [config wireless-controller hotspot20 anqp-venue-name on page 1574](#)
- [config wireless-controller hotspot20 h2qp-conn-capability on page 1575](#)
- [config wireless-controller hotspot20 h2qp-operator-name on page 1577](#)
- [config wireless-controller hotspot20 h2qp-osu-provider on page 1578](#)
- [config wireless-controller hotspot20 h2qp-wan-metric on page 1580](#)
- [config wireless-controller hotspot20 hs-profile on page 1581](#)
- [config wireless-controller hotspot20 icon on page 1588](#)
- [config wireless-controller hotspot20 qos-map on page 1590](#)
- [config wireless-controller inter-controller on page 1591](#)
- [config wireless-controller log on page 1593](#)
- [config wireless-controller qos-profile on page 1597](#)
- [config wireless-controller region on page 1601](#)
- [config wireless-controller setting on page 1602](#)
- [config wireless-controller snmp on page 1608](#)
- [config wireless-controller timers on page 1612](#)
- [config wireless-controller utm-profile on page 1614](#)
- [config wireless-controller vap-group on page 1639](#)
- [config wireless-controller vap on page 1615](#)
- [config wireless-controller wag-profile on page 1640](#)
- [config wireless-controller wids-profile on page 1641](#)
- [config wireless-controller wtp-group on page 1669](#)
- [config wireless-controller wtp-profile on page 1672](#)
- [config wireless-controller wtp on page 1649](#)

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
id	ID.	string	Maximum length: 35
mac	MAC address.	mac-address	Not Specified
policy	Allow or block the client with this MAC address.	option	-

Option	Description
<i>allow</i>	Allow the client with this MAC address.
<i>deny</i>	Block the client with this MAC address.

config wireless-controller addrgrp

Configure the MAC address group.

```
config wireless-controller addrgrp
  Description: Configure the MAC address group.
  edit <id>
    set addresses <id1>, <id2>, ...
    set default-policy [allow|deny]
  next
end
```

config wireless-controller addrgrp

Parameter	Description	Type	Size
addresses <id>	Manually selected group of addresses. Address ID.	string	Maximum length: 35

Parameter	Description	Type	Size
default-policy	Allow or block the clients with MAC addresses that are not in the group.	option	-
	Option	Description	
	<i>allow</i>	Allow the clients with MAC addresses that are not in the group.	
	<i>deny</i>	Block the clients with MAC addresses that are not in the group.	
id	ID.	string	Maximum length: 35

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
id	AP ID.	integer	Minimum value: 0 Maximum value: 4294967295
ssid	Access Point's (AP's) SSID.	string	Maximum length: 32
status	Access Point's (AP's) status: rogue, accepted, or suppressed.	option	-
	Option	Description	
	<i>rogue</i>	Rogue AP.	
	<i>accepted</i>	Accepted AP.	
	<i>suppressed</i>	Suppressed AP.	

config wireless-controller ble-profile

Configure Bluetooth Low Energy profile.

```
config wireless-controller ble-profile
  Description: Configure Bluetooth Low Energy profile.
  edit <name>
    set advertising {option1}, {option2}, ...
    set beacon-interval {integer}
    set ble-scanning [enable|disable]
    set comment {string}
    set eddystone-instance {string}
    set eddystone-namespace {string}
    set eddystone-url {string}
    set ibeacon-uuid {string}
    set major-id {integer}
    set minor-id {integer}
    set txpower [0|1|...]
  next
end
```

config wireless-controller ble-profile

Parameter	Description	Type	Size
advertising	Advertising type.	option	-
	Option	Description	
	ibeacon	iBeacon advertising.	
	eddystone-uid	Eddystone UID advertising.	
	eddystone-url	Eddystone URL advertising.	
beacon-interval	Beacon interval (default = 100 msec).	integer	Minimum value: 40 Maximum value: 3500
ble-scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.	option	-
	Option	Description	
	enable	Enable BLE scanning.	
	disable	Disable BLE scanning.	
comment	Comment.	string	Maximum length: 63
eddystone-instance	Eddystone instance ID.	string	Maximum length: 6

Parameter	Description	Type	Size
eddystone-namespace	Eddystone namespace ID.	string	Maximum length: 10
eddystone-url	Eddystone URL.	string	Maximum length: 127
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
name	Bluetooth Low Energy profile name.	string	Maximum length: 35
txpower	Transmit power level (default = 0).	option	-

Option	Description
0	Transmit power level 0 (-21 dBm)
1	Transmit power level 1 (-18 dBm)
2	Transmit power level 2 (-15 dBm)
3	Transmit power level 3 (-12 dBm)
4	Transmit power level 4 (-9 dBm)
5	Transmit power level 5 (-6 dBm)
6	Transmit power level 6 (-3 dBm)
7	Transmit power level 7 (0 dBm)
8	Transmit power level 8 (1 dBm)
9	Transmit power level 9 (2 dBm)
10	Transmit power level 10 (3 dBm)
11	Transmit power level 11 (4 dBm)
12	Transmit power level 12 (5 dBm)

config wireless-controller bonjour-profile

Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour.

```
config wireless-controller bonjour-profile
    Description: Configure Bonjour profiles. Bonjour is Apple's zero configuration
networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using
Bonjour.
    edit <name>
        set comment {string}
        config policy-list
            Description: Bonjour policy list.
            edit <policy-id>
                set description {string}
                set from-vlan {string}
                set services {option1}, {option2}, ...
                set to-vlan {string}
            next
        end
    next
end
```

config wireless-controller bonjour-profile

Parameter	Description	Type	Size
comment	Comment.	string	Maximum length: 63
name	Bonjour profile name.	string	Maximum length: 35

config policy-list

Parameter	Description	Type	Size
description	Description.	string	Maximum length: 63
from-vlan	VLAN ID from which the Bonjour service is advertised (0 - 4094, default = 0).	string	Maximum length: 63
policy-id	Policy ID.	integer	Minimum value: 1 Maximum value: 65535
services	Bonjour services for the VLAN connecting to the Bonjour network.	option	-

Parameter	Description	Type	Size																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>All services.</td></tr><tr><td><i>airplay</i></td><td>AirPlay.</td></tr><tr><td><i>afp</i></td><td>AFP (Apple File Sharing).</td></tr><tr><td><i>bit-torrent</i></td><td>BitTorrent.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>ichat</i></td><td>iChat.</td></tr><tr><td><i>itunes</i></td><td>iTunes.</td></tr><tr><td><i>printers</i></td><td>Printers.</td></tr><tr><td><i>samba</i></td><td>Samba.</td></tr><tr><td><i>scanners</i></td><td>Scanners.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr><tr><td><i>chromecast</i></td><td>ChromeCast.</td></tr></table>	Option	Description	<i>all</i>	All services.	<i>airplay</i>	AirPlay.	<i>afp</i>	AFP (Apple File Sharing).	<i>bit-torrent</i>	BitTorrent.	<i>ftp</i>	FTP.	<i>ichat</i>	iChat.	<i>itunes</i>	iTunes.	<i>printers</i>	Printers.	<i>samba</i>	Samba.	<i>scanners</i>	Scanners.	<i>ssh</i>	SSH.	<i>chromecast</i>	ChromeCast.		
	Option	Description																											
	<i>all</i>	All services.																											
	<i>airplay</i>	AirPlay.																											
	<i>afp</i>	AFP (Apple File Sharing).																											
	<i>bit-torrent</i>	BitTorrent.																											
	<i>ftp</i>	FTP.																											
	<i>ichat</i>	iChat.																											
	<i>itunes</i>	iTunes.																											
	<i>printers</i>	Printers.																											
	<i>samba</i>	Samba.																											
	<i>scanners</i>	Scanners.																											
	<i>ssh</i>	SSH.																											
<i>chromecast</i>	ChromeCast.																												
to-vlan	VLAN ID to which the Bonjour service is made available (0 - 4094, default = all).	string	Maximum length: 63																										

config wireless-controller global

Configure wireless controller global settings.

```

config wireless-controller global
    Description: Configure wireless controller global settings.
    set ap-log-server [enable|disable]
    set ap-log-server-ip {ipv4-address}
    set ap-log-server-port {integer}
    set control-message-offload {option1}, {option2}, ...
    set data-ethernet-II [enable|disable]
    set discovery-mc-addr {ipv4-address-multicast}
    set fiapp-eth-type {integer}
    set image-download [enable|disable]
    set ipsec-base-ip {ipv4-address}
    set link-aggregation [enable|disable]
    set local-radio-vdom {string}
    set location {string}
    set max-clients {integer}
    set max-retransmit {integer}
    set mesh-eth-type {integer}
    set name {string}
    set rogue-scan-mac-adjacency {integer}
    set wtp-share [enable|disable]
end

```

config wireless-controller global

Parameter	Description	Type	Size
ap-log-server	Enable/disable configuring APs or FortiAPs to send log messages to a syslog server (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable AP log server.	
	<i>disable</i>	Disable AP log server.	
ap-log-server-ip	IP address that APs or FortiAPs send log messages to.	ipv4-address	Not Specified
ap-log-server-port	Port that APs or FortiAPs send log messages to.	integer	Minimum value: 0 Maximum value: 65535
control-message-offload	Configure CAPWAP control message data channel offload.	option	-
	Option	Description	
	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.	
	<i>aeroscout-tag</i>	AeroScout tag.	
	<i>ap-list</i>	Rogue AP list.	
	<i>sta-list</i>	Rogue STA list.	
	<i>sta-cap-list</i>	STA capability list.	
	<i>stats</i>	WTP, radio, VAP, and STA statistics.	
	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	
	<i>sta-health</i>	STA health log.	
data-ethernet-II	Configure the wireless controller to use Ethernet II or 802.3 frames with 802.3 data tunnel mode (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.	
	<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.	
discovery-mc-addr	Multicast IP address for AP discovery (default = 244.0.1.140).	ipv4-address-multicast	Not Specified

Parameter	Description	Type	Size						
fiapp-eth-type	Ethernet type for Fortinet Inter-Access Point Protocol (IAPP), or IEEE 802.11f, packets (0 - 65535, default = 5252).	integer	Minimum value: 5252 Maximum value: 5252						
image-download	Enable/disable WTP image download at join time.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WTP image download at join time.</td></tr><tr><td><i>disable</i></td><td>Disable WTP image download at join time.</td></tr></table>	Option	Description	<i>enable</i>	Enable WTP image download at join time.	<i>disable</i>	Disable WTP image download at join time.		
Option	Description								
<i>enable</i>	Enable WTP image download at join time.								
<i>disable</i>	Disable WTP image download at join time.								
ipsec-base-ip	Base IP address for IPsec VPN tunnels between the access points and the wireless controller (default = 169.254.0.1).	ipv4-address	Not Specified						
link-aggregation	Enable/disable calculating the CAPWAP transmit hash to load balance sessions to link aggregation nodes (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable calculating the CAPWAP transmit hash.</td></tr><tr><td><i>disable</i></td><td>Disable calculating the CAPWAP transmit hash.</td></tr></table>	Option	Description	<i>enable</i>	Enable calculating the CAPWAP transmit hash.	<i>disable</i>	Disable calculating the CAPWAP transmit hash.		
Option	Description								
<i>enable</i>	Enable calculating the CAPWAP transmit hash.								
<i>disable</i>	Disable calculating the CAPWAP transmit hash.								
local-radio-vdom *	Assign local radio's virtual domain.	string	Maximum length: 31						
location	Description of the location of the wireless controller.	string	Maximum length: 35						
max-clients	Maximum number of clients that can connect simultaneously (default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 4294967295						
max-retransmit	Maximum number of tunnel packet retransmissions (0 - 64, default = 3).	integer	Minimum value: 0 Maximum value: 64						
mesh-eth-type *	Mesh Ethernet identifier included in backhaul packets (0 - 65535, default = 8755).	integer	Minimum value: 8755 Maximum value: 8755						
name	Name of the wireless controller.	string	Maximum length: 35						

Parameter	Description	Type	Size
rogue-scan-mac-adjacency	Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection (0 - 31, default = 7).	integer	Minimum value: 0 Maximum value: 31
wtp-share	Enable/disable sharing of WTPs between VDOMs.	option	-

Option	Description
<i>enable</i>	WTP can be shared between all VDOMs.
<i>disable</i>	WTP can be used only in its own VDOM.

* This parameter may not exist in some models.

config wireless-controller hotspot20 anqp-3gpp-cellular

Configure 3GPP public land mobile network (PLMN).

```
config wireless-controller hotspot20 anqp-3gpp-cellular
  Description: Configure 3GPP public land mobile network (PLMN).
  edit <name>
    config mcc-mnc-list
      Description: Mobile Country Code and Mobile Network Code configuration.
      edit <id>
        set mcc {string}
        set mnc {string}
      next
    end
  next
end
```

config wireless-controller hotspot20 anqp-3gpp-cellular

Parameter	Description	Type	Size
name	3GPP PLMN name.	string	Maximum length: 35

config mcc-mnc-list

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 1 Maximum value: 6

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 ipv4-address-type [not-available|public|...]
    set ipv6-address-type [not-available|available|...]
  next
end
```

config wireless-controller hotspot20 anqp-ip-address-type

Parameter	Description	Type	Size
ipv4-address-type	IPv4 address type.	option	-

Option	Description
<i>not-available</i>	Address type not available.
<i>public</i>	Public IPv4 address available.
<i>port-restricted</i>	Port-restricted IPv4 address available.
<i>single-NATed-private</i>	Single NATed private IPv4 address available.
<i>double-NATed-private</i>	Double NATed private IPv4 address available.
<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.
<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.
<i>not-known</i>	Availability of the address type is not known.

Parameter	Description	Type	Size
ipv6-address-type	IPv6 address type.	option	-
	Option	Description	
	<i>not-available</i>	Address type not available.	
	<i>available</i>	Address type available.	
	<i>not-known</i>	Availability of the address type not known.	
name	IP type name.	string	Maximum length: 35

config wireless-controller hotspot20 anqp-nai-realm

Configure network access identifier (NAI) realm.

```

config wireless-controller hotspot20 anqp-nai-realm
  Description: Configure network access identifier (NAI) realm.
  edit <name>
    config nai-list
      Description: NAI list.
      edit <name>
        config eap-method
          Description: EAP Methods.
          edit <index>
            config auth-param
              Description: EAP auth param.
              edit <index>
                set id [non-eap-inner-auth|inner-auth-eap|...]
                set val [eap-identity|eap-md5|...]
              next
            end
            set method [eap-identity|eap-md5|...]
          next
        end
        set encoding [disable|enable]
        set nai-realm {string}
      next
    end
  next
end

```

config wireless-controller hotspot20 anqp-nai-realm

Parameter	Description	Type	Size
name	NAI realm list name.	string	Maximum length: 35

config nai-list

Parameter	Description	Type	Size
encoding	Enable/disable format in accordance with IETF RFC 4282.	option	-
	Option	Description	
	<i>disable</i>	Disable format in accordance with IETF RFC 4282.	
	<i>enable</i>	Enable format in accordance with IETF RFC 4282.	
nai-realm	Configure NAI realms (delimited by a semi-colon character).	string	Maximum length: 255
name	NAI realm name.	string	Maximum length: 35

config eap-method

Parameter	Description	Type	Size
index	EAP method index.	integer	Minimum value: 1 Maximum value: 5
method	EAP method type.	option	-
	Option	Description	
	<i>eap-identity</i>	Identity.	
	<i>eap-md5</i>	MD5.	
	<i>eap-tls</i>	TLS.	
	<i>eap-ttls</i>	TTLS.	
	<i>eap-peap</i>	PEAP.	
	<i>eap-sim</i>	SIM.	
	<i>eap-aka</i>	AKA.	
	<i>eap-aka-prime</i>	AKA'.	

config auth-param

Parameter	Description	Type	Size
id	ID of authentication parameter.	option	-

Parameter	Description	Type	Size

Option	Description
<i>non-eap-inner-auth</i>	Non-EAP inner authentication type.
<i>inner-auth-eap</i>	Inner authentication EAP method type.
<i>credential</i>	Credential type.
<i>tunneled-credential</i>	Tunneled EAP method credential type.

index	Param index.	integer	Minimum value: 1 Maximum value: 4
val	Value of authentication parameter.	option	-

Option	Description
<i>eap-identity</i>	EAP Identity.
<i>eap-md5</i>	EAP MD5.
<i>eap-tls</i>	EAP TLS.
<i>eap-ttls</i>	EAP TTLS.
<i>eap-peap</i>	EAP PEAP.
<i>eap-sim</i>	EAP SIM.
<i>eap-aka</i>	EAP AKA.
<i>eap-aka-prime</i>	EAP AKA'.
<i>non-eap-pap</i>	Non EAP PAP.
<i>non-eap-chap</i>	Non EAP CHAP.
<i>non-eap-mschap</i>	Non EAP MSCHAP.
<i>non-eap-mschapv2</i>	Non EAP MSCHAPV2.
<i>cred-sim</i>	Credential SIM.
<i>cred-usim</i>	Credential USIM.
<i>cred-nfc</i>	Credential NFC secure element.
<i>cred-hardware-token</i>	Credential hardware token.
<i>cred-softoken</i>	Credential softoken.

Parameter	Description	Type	Size

Option	Description
<i>cred-certificate</i>	Credential certificate.
<i>cred-user-pwd</i>	Credential username password.
<i>cred-none</i>	Credential none.
<i>cred-vendor-specific</i>	Credential vendor specific.
<i>tun-cred-sim</i>	Tunneled credential SIM.
<i>tun-cred-usim</i>	Tunneled credential USIM.
<i>tun-cred-nfc</i>	Tunneled credential NFC secure element.
<i>tun-cred-hardware-token</i>	Tunneled credential hardware token.
<i>tun-cred-softoken</i>	Tunneled credential softoken.
<i>tun-cred-certificate</i>	Tunneled credential certificate.
<i>tun-cred-user-pwd</i>	Tunneled credential username password.
<i>tun-cred-anonymous</i>	Tunneled credential anonymous.
<i>tun-cred-vendor-specific</i>	Tunneled credential vendor specific.

config wireless-controller hotspot20 anqp-network-auth-type

Configure network authentication type.

```
config wireless-controller hotspot20 anqp-network-auth-type
  Description: Configure network authentication type.
  edit <name>
    set auth-type [acceptance-of-terms|online-enrollment|...]
    set url {string}
  next
end
```

config wireless-controller hotspot20 anqp-network-auth-type

Parameter	Description	Type	Size
auth-type	Network authentication type.	option	-
	Option	Description	
	<i>acceptance-of-terms</i>	Acceptance of terms and conditions.	
	<i>online-enrollment</i>	Online enrollment supported.	
	<i>http-redirection</i>	HTTP and HTTPS redirection.	
	<i>dns-redirection</i>	DNS redirection.	
name	Authentication type name.	string	Maximum length: 35
url	Redirect URL.	string	Maximum length: 255

config wireless-controller hotspot20 anqp-roaming-consortium

Configure roaming consortium.

```
config wireless-controller hotspot20 anqp-roaming-consortium
  Description: Configure roaming consortium.
  edit <name>
    config oi-list
      Description: Organization identifier list.
      edit <index>
        set comment {string}
        set oi {string}
      next
    end
  next
end
```

config wireless-controller hotspot20 anqp-roaming-consortium

Parameter	Description	Type	Size
name	Roaming consortium name.	string	Maximum length: 35

config oi-list

Parameter	Description	Type	Size
comment	Comment.	string	Maximum length: 35
index	OI index.	integer	Minimum value: 1 Maximum value: 10
oi	Organization identifier.	string	Maximum length: 10

config wireless-controller hotspot20 anqp-venue-name

Configure venue name duple.

```
config wireless-controller hotspot20 anqp-venue-name
  Description: Configure venue name duple.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end
```

config wireless-controller hotspot20 anqp-venue-name

Parameter	Description	Type	Size
name	Name of venue name duple.	string	Maximum length: 35

config value-list

Parameter	Description	Type	Size
index	Value index.	integer	Minimum value: 1 Maximum value: 10

Parameter	Description	Type	Size
lang	Language code.	string	Maximum length: 3
value	Venue name value.	string	Maximum length: 252

config wireless-controller hotspot20 h2qp-conn-capability

Configure connection capability.

```
config wireless-controller hotspot20 h2qp-conn-capability
  Description: Configure connection capability.
  edit <name>
    set esp-port [closed|open|...]
    set ftp-port [closed|open|...]
    set http-port [closed|open|...]
    set icmp-port [closed|open|...]
    set ikev2-port [closed|open|...]
    set ikev2-xx-port [closed|open|...]
    set pptp-vpn-port [closed|open|...]
    set ssh-port [closed|open|...]
    set tls-port [closed|open|...]
    set voip-tcp-port [closed|open|...]
    set voip-udp-port [closed|open|...]
  next
end
```

config wireless-controller hotspot20 h2qp-conn-capability

Parameter	Description	Type	Size
esp-port	Set ESP port service (used by IPsec VPNs) status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
ftp-port	Set FTP port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	

Parameter	Description	Type	Size
http-port	Set HTTP port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
icmp-port	Set ICMP port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
ikev2-port	Set IKEv2 port service for IPsec VPN status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
ikev2-xx-port	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
name	Connection capability name.	string	Maximum length: 35
pptp-vpn-port	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	

Parameter	Description	Type	Size
ssh-port	Set SSH port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
tls-port	Set TLS VPN (HTTPS) port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
voip-tcp-port	Set VoIP TCP port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	
voip-udp-port	Set VoIP UDP port service status.	option	-
	Option	Description	
	<i>closed</i>	The port is not open for communication.	
	<i>open</i>	The port is open for communication.	
	<i>unknown</i>	The port may or may not be open for communication.	

config wireless-controller hotspot20 h2qp-operator-name

Configure operator friendly name.

```
config wireless-controller hotspot20 h2qp-operator-name
  Description: Configure operator friendly name.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
```

```
next
end
```

config wireless-controller hotspot20 h2qp-operator-name

Parameter	Description	Type	Size
name	Friendly name ID.	string	Maximum length: 35

config value-list

Parameter	Description	Type	Size
index	Value index.	integer	Minimum value: 1 Maximum value: 10
lang	Language code.	string	Maximum length: 3
value	Friendly name value.	string	Maximum length: 252

config wireless-controller hotspot20 h2qp-osu-provider

Configure online sign up (OSU) provider list.

```
config wireless-controller hotspot20 h2qp-osu-provider
  Description: Configure online sign up (OSU) provider list.
  edit <name>
    config friendly-name
      Description: OSU provider friendly name.
      edit <index>
        set friendly-name {string}
        set lang {string}
      next
    end
    set icon {string}
    set osu-method {option1}, {option2}, ...
    set osu-nai {string}
    set server-uri {string}
    config service-description
      Description: OSU service name.
      edit <service-id>
        set lang {string}
        set service-description {string}
      next
    end
```

```
next
end
```

config wireless-controller hotspot20 h2qp-osu-provider

Parameter	Description	Type	Size
icon	OSU provider icon.	string	Maximum length: 35
name	OSU provider ID.	string	Maximum length: 35
osu-method	OSU method list.	option	-
	Option	Description	
	<i>oma-dm</i>	OMA DM.	
	<i>soap-xml-spp</i>	SOAP XML SPP.	
	<i>reserved</i>	Reserved.	
osu-nai	OSU NAI.	string	Maximum length: 255
server-uri	Server URI.	string	Maximum length: 255

config friendly-name

Parameter	Description	Type	Size
friendly-name	OSU provider friendly name.	string	Maximum length: 252
index	OSU provider friendly name index.	integer	Minimum value: 1 Maximum value: 10
lang	Language code.	string	Maximum length: 3

config service-description

Parameter	Description	Type	Size
lang	Language code.	string	Maximum length: 3
service-description	Service description.	string	Maximum length: 252

Parameter	Description	Type	Size
service-id	OSU service ID.	integer	Minimum value: 0 Maximum value: 4294967295

config wireless-controller hotspot20 h2qp-wan-metric

Configure WAN metrics.

```
config wireless-controller hotspot20 h2qp-wan-metric
  Description: Configure WAN metrics.
  edit <name>
    set downlink-load {integer}
    set downlink-speed {integer}
    set link-at-capacity [enable|disable]
    set link-status [up|down|...]
    set load-measurement-duration {integer}
    set symmetric-wan-link [symmetric|asymmetric]
    set uplink-load {integer}
    set uplink-speed {integer}
  next
end
```

config wireless-controller hotspot20 h2qp-wan-metric

Parameter	Description	Type	Size
downlink-load	Downlink load.	integer	Minimum value: 0 Maximum value: 255
downlink-speed	Downlink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295
link-at-capacity	Link at capacity.	option	-
	Option	Description	
	enable	Link at capacity (not allow additional mobile devices to associate).	
	disable	Link not at capacity (allow additional mobile devices to associate).	
link-status	Link status.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>up</i>	Link up.	
	<i>down</i>	Link down.	
	<i>in-test</i>	Link in test state.	
load-measurement-duration	Load measurement duration (in tenths of a second).	integer	Minimum value: 0 Maximum value: 65535
name	WAN metric name.	string	Maximum length: 35
symmetric-wan-link	WAN link symmetry.	option	-
	Option	Description	
	<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).	
	<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).	
uplink-load	Uplink load.	integer	Minimum value: 0 Maximum value: 255
uplink-speed	Uplink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295

config wireless-controller hotspot20 hs-profile

Configure hotspot profile.

```
config wireless-controller hotspot20 hs-profile
  Description: Configure hotspot profile.
  edit <name>
    set 3gpp-plmn {string}
    set access-network-asra [enable|disable]
    set access-network-esr [enable|disable]
    set access-network-internet [enable|disable]
    set access-network-type [private-network|private-network-with-guest-access|...]
    set access-network-uesa [enable|disable]
    set anqp-domain-id {integer}
    set bss-transition [enable|disable]
    set conn-cap {string}
```

```

set deauth-request-timeout {integer}
set dgaf [enable|disable]
set domain-name {string}
set gas-comeback-delay {integer}
set gas-fragmentation-limit {integer}
set hessid {mac-address}
set ip-addr-type {string}
set l2tif [enable|disable]
set nai-realm {string}
set network-auth {string}
set oper-friendly-name {string}
set osu-provider <name1>, <name2>, ...
set osu-ssid {string}
set pame-bi [disable|enable]
set proxy-arp [enable|disable]
set qos-map {string}
set roaming-consortium {string}
set venue-group [unspecified|assembly|...]
set venue-name {string}
set venue-type [unspecified|arena|...]
set wan-metrics {string}
set wnm-sleep-mode [enable|disable]
next
end

```

config wireless-controller hotspot20 hs-profile

Parameter	Description	Type	Size						
3gpp-plmn	3GPP PLMN name.	string	Maximum length: 35						
access-network-asra	Enable/disable additional step required for access (ASRA).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable additional step required for access (ASRA).</td></tr><tr><td><i>disable</i></td><td>Disable additional step required for access (ASRA).</td></tr></table>	Option	Description	<i>enable</i>	Enable additional step required for access (ASRA).	<i>disable</i>	Disable additional step required for access (ASRA).		
Option	Description								
<i>enable</i>	Enable additional step required for access (ASRA).								
<i>disable</i>	Disable additional step required for access (ASRA).								
access-network-esr	Enable/disable emergency services reachable (ESR).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable emergency services reachable (ESR).</td></tr><tr><td><i>disable</i></td><td>Disable emergency services reachable (ESR).</td></tr></table>	Option	Description	<i>enable</i>	Enable emergency services reachable (ESR).	<i>disable</i>	Disable emergency services reachable (ESR).		
Option	Description								
<i>enable</i>	Enable emergency services reachable (ESR).								
<i>disable</i>	Disable emergency services reachable (ESR).								
access-network-internet	Enable/disable connectivity to the Internet.	option	-						

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable connectivity to the Internet.</td></tr><tr><td><i>disable</i></td><td>Disable connectivity to the Internet.</td></tr></table>	Option	Description	<i>enable</i>	Enable connectivity to the Internet.	<i>disable</i>	Disable connectivity to the Internet.														
	Option	Description																			
	<i>enable</i>	Enable connectivity to the Internet.																			
<i>disable</i>	Disable connectivity to the Internet.																				
access-network-type	Access network type.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>private-network</i></td><td>Private network.</td></tr><tr><td><i>private-network-with-guest-access</i></td><td>Private network with guest access.</td></tr><tr><td><i>chargeable-public-network</i></td><td>Chargeable public network.</td></tr><tr><td><i>free-public-network</i></td><td>Free public network.</td></tr><tr><td><i>personal-device-network</i></td><td>Personal devices network.</td></tr><tr><td><i>emergency-services-only-network</i></td><td>Emergency services only network.</td></tr><tr><td><i>test-or-experimental</i></td><td>Test or experimental.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard.</td></tr></table>	Option	Description	<i>private-network</i>	Private network.	<i>private-network-with-guest-access</i>	Private network with guest access.	<i>chargeable-public-network</i>	Chargeable public network.	<i>free-public-network</i>	Free public network.	<i>personal-device-network</i>	Personal devices network.	<i>emergency-services-only-network</i>	Emergency services only network.	<i>test-or-experimental</i>	Test or experimental.	<i>wildcard</i>	Wildcard.		
	Option	Description																			
	<i>private-network</i>	Private network.																			
	<i>private-network-with-guest-access</i>	Private network with guest access.																			
	<i>chargeable-public-network</i>	Chargeable public network.																			
	<i>free-public-network</i>	Free public network.																			
	<i>personal-device-network</i>	Personal devices network.																			
	<i>emergency-services-only-network</i>	Emergency services only network.																			
	<i>test-or-experimental</i>	Test or experimental.																			
<i>wildcard</i>	Wildcard.																				
access-network-uesa	Enable/disable unauthenticated emergency service accessible (UESA).	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unauthenticated emergency service accessible (UESA).</td></tr><tr><td><i>disable</i></td><td>Disable unauthenticated emergency service accessible (UESA).</td></tr></table>	Option	Description	<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).	<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).														
	Option	Description																			
	<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).																			
<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).																				
anqp-domain-id	ANQP Domain ID (0-65535).	integer	Minimum value: 0 Maximum value: 65535																		
bss-transition	Enable/disable basic service set (BSS) transition Support.	option	-																		

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable basic service set (BSS) transition support.</td></tr><tr><td><i>disable</i></td><td>Disable basic service set (BSS) transition support.</td></tr></table>	Option	Description	<i>enable</i>	Enable basic service set (BSS) transition support.	<i>disable</i>	Disable basic service set (BSS) transition support.		
	Option	Description							
	<i>enable</i>	Enable basic service set (BSS) transition support.							
<i>disable</i>	Disable basic service set (BSS) transition support.								
conn-cap	Connection capability name.	string	Maximum length: 35						
deauth-request-timeout	Deauthentication request timeout (in seconds).	integer	Minimum value: 30 Maximum value: 120						
dgaf	Enable/disable downstream group-addressed forwarding (DGAF).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable downstream group-addressed forwarding (DGAF).</td></tr><tr><td><i>disable</i></td><td>Disable downstream group-addressed forwarding (DGAF).</td></tr></table>	Option	Description	<i>enable</i>	Enable downstream group-addressed forwarding (DGAF).	<i>disable</i>	Disable downstream group-addressed forwarding (DGAF).		
	Option	Description							
	<i>enable</i>	Enable downstream group-addressed forwarding (DGAF).							
<i>disable</i>	Disable downstream group-addressed forwarding (DGAF).								
domain-name	Domain name.	string	Maximum length: 255						
gas-comeback-delay	GAS comeback delay (0 or 100 - 4000 milliseconds, default = 500).	integer	Minimum value: 100 Maximum value: 4000						
gas-fragmentation-limit	GAS fragmentation limit (512 - 4096, default = 1024).	integer	Minimum value: 512 Maximum value: 4096						
hessid	Homogeneous extended service set identifier (HESSID).	mac-address	Not Specified						
ip-addr-type	IP address type name.	string	Maximum length: 35						
l2tif	Enable/disable Layer 2 traffic inspection and filtering.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Layer 2 traffic inspection and filtering.</td></tr><tr><td><i>disable</i></td><td>Disable Layer 2 traffic inspection and filtering.</td></tr></table>	Option	Description	<i>enable</i>	Enable Layer 2 traffic inspection and filtering.	<i>disable</i>	Disable Layer 2 traffic inspection and filtering.		
	Option	Description							
	<i>enable</i>	Enable Layer 2 traffic inspection and filtering.							
<i>disable</i>	Disable Layer 2 traffic inspection and filtering.								
nai-realm	NAI realm list name.	string	Maximum length: 35						

Parameter	Description	Type	Size
name	Hotspot profile name.	string	Maximum length: 35
network-auth	Network authentication name.	string	Maximum length: 35
oper-friendly-name	Operator friendly name.	string	Maximum length: 35
osu-provider <name>	Manually selected list of OSU provider(s). OSU provider name.	string	Maximum length: 35
osu-ssid	Online sign up (OSU) SSID.	string	Maximum length: 255
pame-bi	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	option	-

Option	Description
<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).
<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).

proxy-arp	Enable/disable Proxy ARP.	option	-

Option	Description
<i>enable</i>	Enable Proxy ARP.
<i>disable</i>	Disable Proxy ARP.

qos-map	QoS MAP set ID.	string	Maximum length: 35

roaming-consortium	Roaming consortium list name.	string	Maximum length: 35

venue-group	Venue group.	option	-

Option	Description
<i>unspecified</i>	Unspecified.
<i>assembly</i>	Assembly.
<i>business</i>	Business.
<i>educational</i>	Educational.
<i>factory</i>	Factory and industrial.

Parameter	Description	Type	Size																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>institutional</i></td><td>Institutional.</td></tr><tr><td><i>mercantile</i></td><td>Mercantile.</td></tr><tr><td><i>residential</i></td><td>Residential.</td></tr><tr><td><i>storage</i></td><td>Storage.</td></tr><tr><td><i>utility</i></td><td>Utility and miscellaneous.</td></tr><tr><td><i>vehicular</i></td><td>Vehicular.</td></tr><tr><td><i>outdoor</i></td><td>Outdoor.</td></tr></table>	Option	Description	<i>institutional</i>	Institutional.	<i>mercantile</i>	Mercantile.	<i>residential</i>	Residential.	<i>storage</i>	Storage.	<i>utility</i>	Utility and miscellaneous.	<i>vehicular</i>	Vehicular.	<i>outdoor</i>	Outdoor.																		
	Option	Description																																	
	<i>institutional</i>	Institutional.																																	
	<i>mercantile</i>	Mercantile.																																	
	<i>residential</i>	Residential.																																	
	<i>storage</i>	Storage.																																	
	<i>utility</i>	Utility and miscellaneous.																																	
	<i>vehicular</i>	Vehicular.																																	
	<i>outdoor</i>	Outdoor.																																	
venue-name	Venue name.	string	Maximum length: 35																																
venue-type	Venue type.	option	-																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unspecified</i></td><td>Unspecified.</td></tr><tr><td><i>arena</i></td><td>Arena.</td></tr><tr><td><i>stadium</i></td><td>Stadium.</td></tr><tr><td><i>passenger-terminal</i></td><td>Passenger terminal.</td></tr><tr><td><i>amphitheater</i></td><td>Amphitheater.</td></tr><tr><td><i>amusement-park</i></td><td>Amusement park.</td></tr><tr><td><i>place-of-worship</i></td><td>Place of worship.</td></tr><tr><td><i>convention-center</i></td><td>Convention center.</td></tr><tr><td><i>library</i></td><td>Library.</td></tr><tr><td><i>museum</i></td><td>Museum.</td></tr><tr><td><i>restaurant</i></td><td>Restaurant.</td></tr><tr><td><i>theater</i></td><td>Theater.</td></tr><tr><td><i>bar</i></td><td>Bar.</td></tr><tr><td><i>coffee-shop</i></td><td>Coffee shop.</td></tr><tr><td><i>zoo-or-aquarium</i></td><td>Zoo or aquarium.</td></tr></table>	Option	Description	<i>unspecified</i>	Unspecified.	<i>arena</i>	Arena.	<i>stadium</i>	Stadium.	<i>passenger-terminal</i>	Passenger terminal.	<i>amphitheater</i>	Amphitheater.	<i>amusement-park</i>	Amusement park.	<i>place-of-worship</i>	Place of worship.	<i>convention-center</i>	Convention center.	<i>library</i>	Library.	<i>museum</i>	Museum.	<i>restaurant</i>	Restaurant.	<i>theater</i>	Theater.	<i>bar</i>	Bar.	<i>coffee-shop</i>	Coffee shop.	<i>zoo-or-aquarium</i>	Zoo or aquarium.		
	Option	Description																																	
	<i>unspecified</i>	Unspecified.																																	
	<i>arena</i>	Arena.																																	
	<i>stadium</i>	Stadium.																																	
	<i>passenger-terminal</i>	Passenger terminal.																																	
	<i>amphitheater</i>	Amphitheater.																																	
	<i>amusement-park</i>	Amusement park.																																	
	<i>place-of-worship</i>	Place of worship.																																	
	<i>convention-center</i>	Convention center.																																	
	<i>library</i>	Library.																																	
	<i>museum</i>	Museum.																																	
	<i>restaurant</i>	Restaurant.																																	
	<i>theater</i>	Theater.																																	
	<i>bar</i>	Bar.																																	
	<i>coffee-shop</i>	Coffee shop.																																	
	<i>zoo-or-aquarium</i>	Zoo or aquarium.																																	

Parameter	Description	Type	Size

Option	Description
<i>emergency-center</i>	Emergency coordination center.
<i>doctor-office</i>	Doctor or dentist office.
<i>bank</i>	Bank.
<i>fire-station</i>	Fire station.
<i>police-station</i>	Police station.
<i>post-office</i>	Post office.
<i>professional-office</i>	Professional office.
<i>research-facility</i>	Research and development facility.
<i>attorney-office</i>	Attorney office.
<i>primary-school</i>	Primary school.
<i>secondary-school</i>	Secondary school.
<i>university-or-college</i>	University or college.
<i>factory</i>	Factory.
<i>hospital</i>	Hospital.
<i>long-term-care-facility</i>	Long term care facility.
<i>rehab-center</i>	Alcohol and drug rehabilitation center.
<i>group-home</i>	Group home.
<i>prison-or-jail</i>	Prison or jail.
<i>retail-store</i>	Retail store.
<i>grocery-market</i>	Grocery market.
<i>auto-service-station</i>	Auto service station.
<i>shopping-mall</i>	Shopping mall.
<i>gas-station</i>	Gas station.
<i>private</i>	Private residence.
<i>hotel-or-motel</i>	Hotel or motel.

Parameter	Description	Type	Size

Option	Description
<i>dormitory</i>	Dormitory.
<i>boarding-house</i>	Boarding house.
<i>automobile</i>	Automobile or truck.
<i>airplane</i>	Airplane.
<i>bus</i>	Bus.
<i>ferry</i>	Ferry.
<i>ship-or-boat</i>	Ship or boat.
<i>train</i>	Train.
<i>motor-bike</i>	Motor bike.
<i>muni-mesh-network</i>	Muni mesh network.
<i>city-park</i>	City park.
<i>rest-area</i>	Rest area.
<i>traffic-control</i>	Traffic control.
<i>bus-stop</i>	Bus stop.
<i>kiosk</i>	Kiosk.

wan-metrics	WAN metric name.	string	Maximum length: 35
wnm-sleep-mode	Enable/disable wireless network management (WNM) sleep mode.	option	-

Option	Description
<i>enable</i>	Enable wireless network management (WNM) sleep mode.
<i>disable</i>	Disable wireless network management (WNM) sleep mode.

config wireless-controller hotspot20 icon

Configure OSU provider icon.

```
config wireless-controller hotspot20 icon
  Description: Configure OSU provider icon.
  edit <name>
    config icon-list
      Description: Icon list.
      edit <name>
```

```

        set file {string}
        set height {integer}
        set lang {string}
        set type [bmp|gif|...]
        set width {integer}
    next
end
next
end

```

config wireless-controller hotspot20 icon

Parameter	Description	Type	Size
name	Icon list ID.	string	Maximum length: 35

config icon-list

Parameter	Description	Type	Size
file	Icon file.	string	Maximum length: 255
height	Icon height.	integer	Minimum value: 1 Maximum value: 65535
lang	Language code.	string	Maximum length: 3
name	Icon name.	string	Maximum length: 255
type	Icon type.	option	-

Option	Description
<i>bmp</i>	BMP image.
<i>gif</i>	GIF image.
<i>jpeg</i>	JPEG image.
<i>png</i>	PNG image.
<i>tiff</i>	TIFF image.

width	Icon width.	integer	Minimum value: 1 Maximum value: 65535

config wireless-controller hotspot20 qos-map

Configure QoS map set.

```
config wireless-controller hotspot20 qos-map
  Description: Configure QoS map set.
  edit <name>
    config dscp-except
      Description: Differentiated Services Code Point (DSCP) exceptions.
      edit <index>
        set dscp {integer}
        set up {integer}
      next
    end
  config dscp-range
    Description: Differentiated Services Code Point (DSCP) ranges.
    edit <index>
      set high {integer}
      set low {integer}
      set up {integer}
    next
  end
next
end
```

config wireless-controller hotspot20 qos-map

Parameter	Description	Type	Size
name	QOS-MAP name.	string	Maximum length: 35

config dscp-except

Parameter	Description	Type	Size
dscp	DSCP value.	integer	Minimum value: 0 Maximum value: 63
index	DSCP exception index.	integer	Minimum value: 1 Maximum value: 21
up	User priority.	integer	Minimum value: 0 Maximum value: 7

config dscp-range

Parameter	Description	Type	Size
high	DSCP high value.	integer	Minimum value: 0 Maximum value: 63
index	DSCP range index.	integer	Minimum value: 1 Maximum value: 8
low	DSCP low value.	integer	Minimum value: 0 Maximum value: 63
up	User priority.	integer	Minimum value: 0 Maximum value: 7

config wireless-controller inter-controller

Configure inter wireless controller operation.

```
config wireless-controller inter-controller
  Description: Configure inter wireless controller operation.
  set fast-failover-max {integer}
  set fast-failover-wait {integer}
  set inter-controller-key {password}
  set inter-controller-mode [disable|l2-roaming|...]
  config inter-controller-peer
    Description: Fast failover peer wireless controller list.
    edit <id>
      set peer-ip {ipv4-address}
      set peer-port {integer}
      set peer-priority [primary|secondary]
    next
  end
  set inter-controller-pri [primary|secondary]
end
```

config wireless-controller inter-controller

Parameter	Description	Type	Size
fast-failover-max	Maximum number of retransmissions for fast failover HA messages between peer wireless controllers (3 - 64, default = 10).	integer	Minimum value: 3 Maximum value: 64
fast-failover-wait	Minimum wait time before an AP transitions from secondary controller to primary controller (10 - 86400 sec, default = 10).	integer	Minimum value: 10 Maximum value: 86400
inter-controller-key	Secret key for inter-controller communications.	password	Not Specified
inter-controller-mode	Configure inter-controller mode (disable, l2-roaming, 1+1, default = disable).	option	-

Option	Description
<i>disable</i>	Disable inter-controller mode.
<i>l2-roaming</i>	Enable layer 2 roaming support between inter-controllers.
<i>1+1</i>	Enable 1+1 fast failover mode.

inter-controller-pri	Configure inter-controller's priority (primary or secondary, default = primary).	option	-

Option	Description
<i>primary</i>	Primary fast failover mode.
<i>secondary</i>	Secondary fast failover mode.

config inter-controller-peer

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
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 (1024 - 49150, default = 5246).	integer	Minimum value: 1024 Maximum value: 49150

Parameter	Description	Type	Size
peer-priority	Peer wireless controller's priority (primary or secondary, default = primary).	option	-
	Option	Description	
	<i>primary</i>	Primary fast failover mode.	
	<i>secondary</i>	Secondary fast failover mode.	

config wireless-controller log

Configure wireless controller event log filters.

```
config wireless-controller log
    Description: Configure wireless controller event log filters.
    set addrgrp-log [emergency|alert|...]
    set ble-log [emergency|alert|...]
    set clb-log [emergency|alert|...]
    set dhcp-starv-log [emergency|alert|...]
    set led-sched-log [emergency|alert|...]
    set radio-event-log [emergency|alert|...]
    set rogue-event-log [emergency|alert|...]
    set sta-event-log [emergency|alert|...]
    set sta-locate-log [emergency|alert|...]
    set status [enable|disable]
    set wids-log [emergency|alert|...]
    set wtp-event-log [emergency|alert|...]
end
```

config wireless-controller log

Parameter	Description	Type	Size
addrgrp-log	Lowest severity level to log address group message.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	

Parameter	Description	Type	Size

Option	Description
<i>debug</i>	Debug level.

ble-log	Lowest severity level to log BLE detection message.	option	-

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

clb-log	Lowest severity level to log client load balancing message.	option	-

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

dhcp-starv-log	Lowest severity level to log DHCP starvation event message.	option	-

Option	Description
<i>emergency</i>	Emergency level.
<i>alert</i>	Alert level.
<i>critical</i>	Critical level.

Parameter	Description	Type	Size

Option		Description
	<i>error</i>	Error level.
	<i>warning</i>	Warning level.
	<i>notification</i>	Notification level.
	<i>information</i>	Information level.
	<i>debug</i>	Debug level.

led-sched-log	Lowest severity level to log LED schedule event message.	option	-

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

radio-event-log	Lowest severity level to log radio event message.	option	-

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

rogue-event-log	Lowest severity level to log rogue AP event message.	option	-

Parameter	Description	Type	Size

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

sta-event-log	Lowest severity level to log station event message.	option	-

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

sta-locate-log	Lowest severity level to log station locate message.	option	-

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

Parameter	Description	Type	Size
status	Enable/disable wireless event logging.	option	-
	Option	Description	
	<i>enable</i>	Enable wireless event logging.	
	<i>disable</i>	Disable wireless event logging.	
wids-log	Lowest severity level to log WIDS message.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	
wtp-event-log	Lowest severity level to log WTP event message.	option	-
	Option	Description	
	<i>emergency</i>	Emergency level.	
	<i>alert</i>	Alert level.	
	<i>critical</i>	Critical level.	
	<i>error</i>	Error level.	
	<i>warning</i>	Warning level.	
	<i>notification</i>	Notification level.	
	<i>information</i>	Information level.	
	<i>debug</i>	Debug level.	

config wireless-controller qos-profile

Configure WiFi quality of service (QoS) profiles.

```
config wireless-controller qos-profile
  Description: Configure WiFi quality of service (QoS) profiles.
  edit <name>
    set bandwidth-admission-control [enable|disable]
```

```

set bandwidth-capacity {integer}
set burst [enable|disable]
set call-admission-control [enable|disable]
set call-capacity {integer}
set comment {string}
set downlink {integer}
set downlink-sta {integer}
set dscp-wmm-be <id1>, <id2>, ...
set dscp-wmm-bk <id1>, <id2>, ...
set dscp-wmm-mapping [enable|disable]
set dscp-wmm-vi <id1>, <id2>, ...
set dscp-wmm-vo <id1>, <id2>, ...
set uplink {integer}
set uplink-sta {integer}
set wmm [enable|disable]
set wmm-be-dscp {integer}
set wmm-bk-dscp {integer}
set wmm-dscp-marking [enable|disable]
set wmm-uapsd [enable|disable]
set wmm-vi-dscp {integer}
set wmm-vo-dscp {integer}
next
end

```

config wireless-controller qos-profile

Parameter	Description	Type	Size						
bandwidth-admission-control	Enable/disable WMM bandwidth admission control.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.		
Option	Description								
<i>enable</i>	Enable WMM bandwidth admission control.								
<i>disable</i>	Disable WMM bandwidth admission control.								
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000						
burst	Enable/disable client rate burst.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable client rate burst.</td></tr><tr><td><i>disable</i></td><td>Disable client rate burst.</td></tr></table>	Option	Description	<i>enable</i>	Enable client rate burst.	<i>disable</i>	Disable client rate burst.		
Option	Description								
<i>enable</i>	Enable client rate burst.								
<i>disable</i>	Disable client rate burst.								

Parameter	Description	Type	Size						
call-admission-control	Enable/disable WMM call admission control.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.		
Option	Description								
<i>enable</i>	Enable WMM call admission control.								
<i>disable</i>	Disable WMM call admission control.								
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones allowed (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60						
comment	Comment.	string	Maximum length: 63						
downlink	Maximum downlink bandwidth for Virtual Access Points (VAPs) (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152						
downlink-sta	Maximum downlink bandwidth for clients (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152						
dscp-wmm-be<id>	DSCP mapping for best effort access (default = 0 24). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63						
dscp-wmm-bk<id>	DSCP mapping for background access (default = 8 16). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63						
dscp-wmm-mapping	Enable/disable Differentiated Services Code Point (DSCP) mapping.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Differentiated Services Code Point (DSCP) mapping.</td></tr><tr><td><i>disable</i></td><td>Disable Differentiated Services Code Point (DSCP) mapping.</td></tr></table>	Option	Description	<i>enable</i>	Enable Differentiated Services Code Point (DSCP) mapping.	<i>disable</i>	Disable Differentiated Services Code Point (DSCP) mapping.		
Option	Description								
<i>enable</i>	Enable Differentiated Services Code Point (DSCP) mapping.								
<i>disable</i>	Disable Differentiated Services Code Point (DSCP) mapping.								
dscp-wmm-vi<id>	DSCP mapping for video access (default = 32 40). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63						

Parameter	Description	Type	Size						
dscp-wmm-vo <id>	DSCP mapping for voice access (default = 48 56). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63						
name	WiFi QoS profile name.	string	Maximum length: 35						
uplink	Maximum uplink bandwidth for Virtual Access Points (VAPs) (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152						
uplink-sta	Maximum uplink bandwidth for clients (0 - 2097152 Kbps, default = 0, 0 means no limit).	integer	Minimum value: 0 Maximum value: 2097152						
wmm	Enable/disable WiFi multi-media (WMM) control.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WiFi multi-media (WMM) control.</td></tr><tr><td>disable</td><td>Disable WiFi multi-media (WMM) control.</td></tr></table>			Option	Description	enable	Enable WiFi multi-media (WMM) control.	disable	Disable WiFi multi-media (WMM) control.
Option	Description								
enable	Enable WiFi multi-media (WMM) control.								
disable	Disable WiFi multi-media (WMM) control.								
wmm-be-dscp	DSCP marking for best effort access (default = 0).	integer	Minimum value: 0 Maximum value: 63						
wmm-bk-dscp	DSCP marking for background access (default = 8).	integer	Minimum value: 0 Maximum value: 63						
wmm-dscp-marking	Enable/disable WMM Differentiated Services Code Point (DSCP) marking.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM Differentiated Services Code Point (DSCP) marking.</td></tr><tr><td>disable</td><td>Disable WMM Differentiated Services Code Point (DSCP) marking.</td></tr></table>			Option	Description	enable	Enable WMM Differentiated Services Code Point (DSCP) marking.	disable	Disable WMM Differentiated Services Code Point (DSCP) marking.
Option	Description								
enable	Enable WMM Differentiated Services Code Point (DSCP) marking.								
disable	Disable WMM Differentiated Services Code Point (DSCP) marking.								
wmm-uapsd	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	option	-						

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	
	<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	
wmm-vi-dscp	DSCP marking for video access (default = 32).	integer	Minimum value: 0 Maximum value: 63
wmm-vo-dscp	DSCP marking for voice access (default = 48).	integer	Minimum value: 0 Maximum value: 63

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable region image grayscale.</td></tr><tr><td><i>disable</i></td><td>Disable region image grayscale.</td></tr></table>			Option	Description	<i>enable</i>	Enable region image grayscale.	<i>disable</i>	Disable region image grayscale.
	Option	Description							
	<i>enable</i>	Enable region image grayscale.							
<i>disable</i>	Disable region image grayscale.								
name	FortiAP region name.	string	Maximum length: 35						

Parameter	Description	Type	Size
opacity	Region image opacity (0 - 100).	integer	Minimum value: 0 Maximum value: 100

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 darrp-optimize {integer}
    set darrp-optimize-schedules <name1>, <name2>, ...
    set duplicate-ssid [enable|disable]
    set fake-ssid-action {option1}, {option2}, ...
    set fapc-compatibility [enable|disable]
    config offending-ssid
        Description: Configure offending SSID.
        edit <id>
            set action {option1}, {option2}, ...
            set ssid-pattern {string}
        next
    end
    set phishing-ssid-detect [enable|disable]
    set wfa-compatibility [enable|disable]
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

Parameter	Description	Type	Size

Option	Description
<i>AO</i>	ANGOLA
<i>AR</i>	ARGENTINA
<i>AM</i>	ARMENIA
<i>AU</i>	AUSTRALIA
<i>AT</i>	AUSTRIA
<i>AZ</i>	AZERBAIJAN
<i>BS</i>	BAHAMAS
<i>BH</i>	BAHRAIN
<i>BD</i>	BANGLADESH
<i>BB</i>	BARBADOS
<i>BY</i>	BELARUS
<i>BE</i>	BELGIUM
<i>BZ</i>	BELIZE
<i>BO</i>	BOLIVIA
<i>BA</i>	BOSNIA AND HERZEGOVINA
<i>BR</i>	BRAZIL
<i>BN</i>	BRUNEI DARUSSALAM
<i>BG</i>	BULGARIA
<i>KH</i>	CAMBODIA
<i>CF</i>	CENTRAL AFRICA REPUBLIC
<i>CL</i>	CHILE
<i>CN</i>	CHINA
<i>CO</i>	COLOMBIA
<i>CR</i>	COSTA RICA
<i>HR</i>	CROATIA
<i>CY</i>	CYPRUS
<i>CZ</i>	CZECH REPUBLIC
<i>DK</i>	DENMARK
<i>DO</i>	DOMINICAN REPUBLIC

Parameter	Description	Type	Size

Option	Description
<i>EC</i>	ECUADOR
<i>EG</i>	EGYPT
<i>SV</i>	EL SALVADOR
<i>EE</i>	ESTONIA
<i>FI</i>	FINLAND
<i>FR</i>	FRANCE
<i>GE</i>	GEORGIA
<i>DE</i>	GERMANY
<i>GR</i>	GREECE
<i>GL</i>	GREENLAND
<i>GD</i>	GRENADA
<i>GU</i>	GUAM
<i>GT</i>	GUATEMALA
<i>HT</i>	HAITI
<i>HN</i>	HONDURAS
<i>HK</i>	HONG KONG
<i>HU</i>	HUNGARY
<i>IS</i>	ICELAND
<i>IN</i>	INDIA
<i>ID</i>	INDONESIA
<i>IR</i>	IRAN
<i>IE</i>	IRELAND
<i>IL</i>	ISRAEL
<i>IT</i>	ITALY
<i>JM</i>	JAMAICA
<i>JO</i>	JORDAN
<i>KZ</i>	KAZAKHSTAN
<i>KE</i>	KENYA
<i>KP</i>	NORTH KOREA

Parameter	Description	Type	Size

Option	Description
<i>KR</i>	KOREA REPUBLIC
<i>KW</i>	KUWAIT
<i>LV</i>	LATVIA
<i>LB</i>	LEBANON
<i>LI</i>	LIECHTENSTEIN
<i>LT</i>	LITHUANIA
<i>LU</i>	LUXEMBOURG
<i>MO</i>	MACAU SAR
<i>MK</i>	MACEDONIA, FYRO
<i>MY</i>	MALAYSIA
<i>MT</i>	MALTA
<i>MX</i>	MEXICO
<i>MC</i>	MONACO
<i>MA</i>	MOROCCO
<i>MZ</i>	MOZAMBIQUE
<i>MM</i>	MYANMAR
<i>NP</i>	NEPAL
<i>NL</i>	NETHERLANDS
<i>AN</i>	NETHERLANDS ANTILLES
<i>AW</i>	ARUBA
<i>NZ</i>	NEW ZEALAND
<i>NO</i>	NORWAY
<i>OM</i>	OMAN
<i>PK</i>	PAKISTAN
<i>PA</i>	PANAMA
<i>PG</i>	PAPUA NEW GUINEA
<i>PY</i>	PARAGUAY
<i>PE</i>	PERU
<i>PH</i>	PHILIPPINES

Parameter	Description	Type	Size

Option	Description
<i>PL</i>	POLAND
<i>PT</i>	PORTUGAL
<i>PR</i>	PUERTO RICO
<i>QA</i>	QATAR
<i>RO</i>	ROMANIA
<i>RU</i>	RUSSIA
<i>RW</i>	RWANDA
<i>SA</i>	SAUDI ARABIA
<i>RS</i>	REPUBLIC OF SERBIA
<i>ME</i>	MONTENEGRO
<i>SG</i>	SINGAPORE
<i>SK</i>	SLOVAKIA
<i>SI</i>	SLOVENIA
<i>ZA</i>	SOUTH AFRICA
<i>ES</i>	SPAIN
<i>LK</i>	SRI LANKA
<i>SE</i>	SWEDEN
<i>SD</i>	SUDAN
<i>CH</i>	SWITZERLAND
<i>SY</i>	SYRIAN ARAB REPUBLIC
<i>TW</i>	TAIWAN
<i>TZ</i>	TANZANIA
<i>TH</i>	THAILAND
<i>TT</i>	TRINIDAD AND TOBAGO
<i>TN</i>	TUNISIA
<i>TR</i>	TURKEY
<i>AE</i>	UNITED ARAB EMIRATES
<i>UA</i>	UKRAINE
<i>GB</i>	UNITED KINGDOM

Parameter	Description	Type	Size

Option	Description
<i>US</i>	UNITED STATES2
<i>PS</i>	UNITED STATES (PUBLIC SAFETY)
<i>UY</i>	URUGUAY
<i>UZ</i>	UZBEKISTAN
<i>VE</i>	VENEZUELA
<i>VN</i>	VIET NAM
<i>YE</i>	YEMEN
<i>ZB</i>	ZAMBIA
<i>ZW</i>	ZIMBABWE
<i>JP</i>	JAPAN14
<i>CA</i>	CANADA2

darrp-optimize	Time for running Dynamic Automatic Radio Resource Provisioning (DARRP) optimizations (0 - 86400 sec, default = 86400, 0 = disable).	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
duplicate-ssid	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.	option	-

Option	Description
<i>enable</i>	Allow VAPs to use the same SSID name in the same VDOM.
<i>disable</i>	Do not allow VAPs to use the same SSID name in the same VDOM.

fake-ssid-action	Actions taken for detected fake SSID.	option	-

Option	Description
<i>log</i>	Write logs for detected fake SSID.
<i>suppress</i>	Suppress detected fake SSID.

Parameter	Description	Type	Size						
fapc-compatibility	Enable/disable FAP-C series compatibility.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FAP-C series compatibility.</td></tr><tr><td><i>disable</i></td><td>Disable FAP-C series compatibility.</td></tr></table>	Option	Description	<i>enable</i>	Enable FAP-C series compatibility.	<i>disable</i>	Disable FAP-C series compatibility.		
Option	Description								
<i>enable</i>	Enable FAP-C series compatibility.								
<i>disable</i>	Disable FAP-C series compatibility.								
phishing-ssid-detect	Enable/disable phishing SSID detection.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phishing SSID detection.</td></tr><tr><td><i>disable</i></td><td>Disable phishing SSID detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable phishing SSID detection.	<i>disable</i>	Disable phishing SSID detection.		
Option	Description								
<i>enable</i>	Enable phishing SSID detection.								
<i>disable</i>	Disable phishing SSID detection.								
wfa-compatibility	Enable/disable WFA compatibility.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Wi-Fi Alliance Certification compatibility.</td></tr><tr><td><i>disable</i></td><td>Disable Wi-Fi Alliance Certification compatibility.</td></tr></table>	Option	Description	<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.	<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.		
Option	Description								
<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.								
<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.								

config offending-ssid

Parameter	Description	Type	Size						
action	Actions taken for detected offending SSID.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>log</i></td><td>Generate logs for detected offending SSID.</td></tr><tr><td><i>suppress</i></td><td>Suppress detected offending SSID.</td></tr></table>	Option	Description	<i>log</i>	Generate logs for detected offending SSID.	<i>suppress</i>	Suppress detected offending SSID.		
	Option	Description							
	<i>log</i>	Generate logs for detected offending SSID.							
<i>suppress</i>	Suppress detected offending SSID.								
id	ID.	integer	Minimum value: 0 Maximum value: 65535						
ssid-pattern	Define offending SSID pattern (case insensitive), eg: word, word*, *word, wo*rd.	string	Maximum length: 33						

config wireless-controller snmp

Configure SNMP.


```

config wireless-controller snmp
  Description: Configure SNMP.
  config community
    Description: SNMP Community Configuration.
    edit <id>
      config hosts
        Description: Configure IPv4 SNMP managers (hosts).
        edit <id>
          set ip {user}
        next
      end
      set name {string}
      set query-v1-status [enable|disable]
      set query-v2c-status [enable|disable]
      set status [enable|disable]
      set trap-v1-status [enable|disable]
      set trap-v2c-status [enable|disable]
    next
  end
  set contact-info {string}
  set engine-id {string}
  set trap-high-cpu-threshold {integer}
  set trap-high-mem-threshold {integer}
  config user
    Description: SNMP User Configuration.
    edit <name>
      set auth-proto [md5|sha]
      set auth-pwd {password}
      set notify-hosts {ipv4-address}
      set priv-proto [aes|des|...]
      set priv-pwd {password}
      set queries [enable|disable]
      set security-level [no-auth-no-priv|auth-no-priv|...]
      set status [enable|disable]
      set trap-status [enable|disable]
    next
  end
end

```

config wireless-controller snmp

Parameter	Description	Type	Size
contact-info	Contact Information.	string	Maximum length: 31
engine-id	AC SNMP engineId string (maximum 24 characters).	string	Maximum length: 23
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100

Parameter	Description	Type	Size
trap-high-mem-threshold	Memory usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100

config community

Parameter	Description	Type	Size
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295
name	Community name.	string	Maximum length: 35
query-v1-status	Enable/disable SNMP v1 queries.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

query-v2c-status	Enable/disable SNMP v2c queries.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

status	Enable/disable this SNMP community.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

trap-v1-status	Enable/disable SNMP v1 traps.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

Parameter	Description	Type	Size
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-

Option	Description
<i>enable</i>	Enable setting.
<i>disable</i>	Disable setting.

config hosts

Parameter	Description	Type	Size
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295
ip	IPv4 address of the SNMP manager (host).	user	Not Specified

config user

Parameter	Description	Type	Size
auth-proto	Authentication protocol.	option	-

Option	Description
<i>md5</i>	HMAC-MD5-96 authentication protocol.
<i>sha</i>	HMAC-SHA-96 authentication protocol.

auth-pwd	Password for authentication protocol.	password	Not Specified
name	SNMP User Name	string	Maximum length: 32
notify-hosts	Configure SNMP User Notify Hosts.	ipv4-address	Not Specified
priv-proto	Privacy (encryption) protocol.	option	-

Option	Description
<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.
<i>des</i>	CBC-DES symmetric encryption protocol.
<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.
<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.

Parameter	Description	Type	Size								
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified								
queries	Enable/disable SNMP queries for this user.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
security-level	Security level for message authentication and encryption.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-auth-no-priv</i></td><td>Message with no authentication and no privacy (encryption).</td></tr><tr><td><i>auth-no-priv</i></td><td>Message with authentication but no privacy (encryption).</td></tr><tr><td><i>auth-priv</i></td><td>Message with authentication and privacy (encryption).</td></tr></table>	Option	Description	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).	<i>auth-priv</i>	Message with authentication and privacy (encryption).		
Option	Description										
<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).										
<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).										
<i>auth-priv</i>	Message with authentication and privacy (encryption).										
status	SNMP User Enable	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										
trap-status	Enable/disable traps for this SNMP user.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
Option	Description										
<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.										

config wireless-controller timers

Configure CAPWAP timers.

```
config wireless-controller timers
  Description: Configure CAPWAP timers.
  set ble-scan-report-intv {integer}
  set client-idle-timeout {integer}
  set discovery-interval {integer}
  set echo-interval {integer}
  set fake-ap-log {integer}
  set ipsec-intf-cleanup {integer}
  set radio-stats-interval {integer}
  set rogue-ap-log {integer}
  set sta-capability-interval {integer}
```

```

set sta-locate-timer {integer}
set sta-stats-interval {integer}
set vap-stats-interval {integer}
end

```

config wireless-controller timers

Parameter	Description	Type	Size
ble-scan-report-intv	Time between running Bluetooth Low Energy (BLE) reports (10 - 3600 sec, default = 30).	integer	Minimum value: 10 Maximum value: 3600
client-idle-timeout	Time after which a client is considered idle and times out (20 - 3600 sec, default = 300, 0 for no timeout).	integer	Minimum value: 20 Maximum value: 3600
discovery-interval	Time between discovery requests (2 - 180 sec, default = 5).	integer	Minimum value: 2 Maximum value: 180
echo-interval	Time between echo requests sent by the managed WTP, AP, or FortiAP (1 - 255 sec, default = 30).	integer	Minimum value: 1 Maximum value: 255
fake-ap-log	Time between recording logs about fake APs if periodic fake AP logging is configured (0 - 1440 min, default = 1).	integer	Minimum value: 1 Maximum value: 1440
ipsec-intf-cleanup	Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected (30 - 3600 sec, default = 120).	integer	Minimum value: 30 Maximum value: 3600
radio-stats-interval	Time between running radio reports (1 - 255 sec, default = 15).	integer	Minimum value: 1 Maximum value: 255
rogue-ap-log	Time between logging rogue AP messages if periodic rogue AP logging is configured (0 - 1440 min, default = 0).	integer	Minimum value: 0 Maximum value: 1440

Parameter	Description	Type	Size
sta-capability-interval	Time between running station capability reports (1 - 255 sec, default = 30).	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 (0 - 86400 sec, default = 1800).	integer	Minimum value: 0 Maximum value: 86400
sta-stats-interval	Time between running client (station) reports (1 - 255 sec, default = 1).	integer	Minimum value: 1 Maximum value: 255
vap-stats-interval	Time between running Virtual Access Point (VAP) reports (1 - 255 sec, default = 15).	integer	Minimum value: 1 Maximum value: 255

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 antivirus-profile {string}
    set application-list {string}
    set comment {string}
    set ips-sensor {string}
    set scan-botnet-connections [disable|monitor|...]
    set utm-log [enable|disable]
    set webfilter-profile {string}
  next
end
```

config wireless-controller utm-profile

Parameter	Description	Type	Size
antivirus-profile	AntiVirus profile name.	string	Maximum length: 35
application-list	Application control list name.	string	Maximum length: 35

Parameter	Description	Type	Size								
comment	Comment.	string	Maximum length: 63								
ips-sensor	IPS sensor name.	string	Maximum length: 35								
name	UTM profile name.	string	Maximum length: 35								
scan-botnet-connections	Block or monitor connections to Botnet servers or disable Botnet scanning.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not scan connections to botnet servers.</td></tr><tr><td><i>monitor</i></td><td>Log connections to botnet servers.</td></tr><tr><td><i>block</i></td><td>Block connections to botnet servers.</td></tr></table>			Option	Description	<i>disable</i>	Do not scan connections to botnet servers.	<i>monitor</i>	Log connections to botnet servers.	<i>block</i>	Block connections to botnet servers.
Option	Description										
<i>disable</i>	Do not scan connections to botnet servers.										
<i>monitor</i>	Log connections to botnet servers.										
<i>block</i>	Block connections to botnet servers.										
utm-log	Enable/disable UTM logging.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable UTM logging.</td></tr><tr><td><i>disable</i></td><td>Disable UTM logging.</td></tr></table>			Option	Description	<i>enable</i>	Enable UTM logging.	<i>disable</i>	Disable UTM logging.		
Option	Description										
<i>enable</i>	Enable UTM logging.										
<i>disable</i>	Disable UTM logging.										
webfilter-profile	WebFilter profile 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 acct-interim-interval {integer}
    set address-group {string}
    set atf-weight {integer}
    set auth [psk|radius|...]
    set broadcast-ssid [enable|disable]
    set broadcast-suppression {option1}, {option2}, ...
    set captive-portal-ac-name {string}
    set captive-portal-macauth-radius-secret {password}
    set captive-portal-macauth-radius-server {string}
    set captive-portal-radius-secret {password}
    set captive-portal-radius-server {string}
    set captive-portal-session-timeout-interval {integer}
    set dhcp-lease-time {integer}
    set dhcp-option82-circuit-id-insertion [style-1|style-2|...]
    set dhcp-option82-insertion [enable|disable]
```

```

set dhcp-option82-remote-id-insertion [style-1|disable]
set dynamic-vlan [enable|disable]
set eap-reauth [enable|disable]
set eap-reauth-intv {integer}
set eapol-key-retries [disable|enable]
set encrypt [TKIP|AES|...]
set external-fast-roaming [enable|disable]
set external-logout {string}
set external-web {string}
set external-web-format [auto-detect|no-query-string|...]
set fast-bss-transition [disable|enable]
set fast-roaming [enable|disable]
set ft-mobility-domain {integer}
set ft-over-ds [disable|enable]
set ft-r0-key-lifetime {integer}
set gtk-rekey [enable|disable]
set gtk-rekey-intv {integer}
set high-efficiency [enable|disable]
set hotspot20-profile {string}
set intra-vap-privacy [enable|disable]
set ip {ipv4-classnet-host}
set key {password}
set keyindex {integer}
set ldpc [disable|rx|...]
set local-authentication [enable|disable]
set local-bridging [enable|disable]
set local-lan [allow|deny]
set local-standalone [enable|disable]
set local-standalone-nat [enable|disable]
set mac-auth-bypass [enable|disable]
set mac-filter [enable|disable]
config mac-filter-list
    Description: Create a list of MAC addresses for MAC address filtering.
    edit <id>
        set mac {mac-address}
        set mac-filter-policy [allow|deny]
    next
end
set mac-filter-policy-other [allow|deny]
set max-clients {integer}
set max-clients-ap {integer}
set me-disable-thresh {integer}
set mesh-backhaul [enable|disable]
set mpsk [enable|disable]
set mpsk-concurrent-clients {integer}
config mpsk-key
    Description: List of multiple PSK entries.
    edit <key-name>
        set comment {var-string}
        set concurrent-clients {string}
        set mpsk-schedules <name1>, <name2>, ...
        set passphrase {password}
    next
end
set mu-mimo [enable|disable]
set multicast-enhance [enable|disable]

```



```

set multicast-rate [0|6000|...]
set okc [disable|enable]
set owe-groups {option1}, {option2}, ...
set owe-transition [disable|enable]
set owe-transition-ssid {string}
set passphrase {password}
set pmf [disable|enable|...]
set pmf-assoc-comeback-timeout {integer}
set pmf-sa-query-retry-timeout {integer}
set port-macauth [disable|radius|...]
set port-macauth-reauth-timeout {integer}
set port-macauth-timeout {integer}
set portal-message-override-group {string}
config portal-message-overrides
    Description: Individual message overrides.
    set auth-disclaimer-page {string}
    set auth-login-failed-page {string}
    set auth-login-page {string}
    set auth-reject-page {string}
end
set portal-type [auth|auth+disclaimer|...]
set primary-wag-profile {string}
set probe-resp-suppression [enable|disable]
set probe-resp-threshold {string}
set ptk-rekey [enable|disable]
set ptk-rekey-intv {integer}
set qos-profile {string}
set quarantine [enable|disable]
set radio-2g-threshold {string}
set radio-5g-threshold {string}
set radio-sensitivity [enable|disable]
set radius-mac-auth [enable|disable]
set radius-mac-auth-server {string}
set radius-mac-auth-usergroups <name1>, <name2>, ...
set radius-server {string}
set rates-11a {option1}, {option2}, ...
set rates-11ac-ss12 {option1}, {option2}, ...
set rates-11ac-ss34 {option1}, {option2}, ...
set rates-11bg {option1}, {option2}, ...
set rates-11n-ss12 {option1}, {option2}, ...
set rates-11n-ss34 {option1}, {option2}, ...
set sae-groups {option1}, {option2}, ...
set sae-password {password}
set schedule <name1>, <name2>, ...
set secondary-wag-profile {string}
set security [open|captive-portal|...]
set security-exempt-list {string}
set security-redirect-url {string}
set selected-usergroups <name1>, <name2>, ...
set split-tunneling [enable|disable]
set ssid {string}
set target-wake-time [enable|disable]
set tkip-counter-measure [enable|disable]
set tunnel-echo-interval {integer}
set tunnel-fallback-interval {integer}
set usergroup <name1>, <name2>, ...

```

```

set utm-profile {string}
set vlan-auto [enable|disable]
config vlan-pool
    Description: VLAN pool.
    edit <id>
        set wtp-group {string}
    next
end
set vlan-pooling [wtp-group|round-robin|...]
set vlanid {integer}
set voice-enterprise [disable|enable]
next
end

```

config wireless-controller vap

Parameter	Description	Type	Size
acct-interim-interval	WiFi RADIUS accounting interim interval (60 - 86400 sec, default = 0).	integer	Minimum value: 60 Maximum value: 86400
address-group	Address group ID.	string	Maximum length: 35
att-weight	Airtime weight in percentage (default = 20).	integer	Minimum value: 0 Maximum value: 100
auth	Authentication protocol.	option	-
	Option	Description	
	<i>psk</i>	Use a single Pre-shared Key (PSK) to authenticate all users.	
	<i>radius</i>	Use a RADIUS server to authenticate clients.	
	<i>usergroup</i>	Use a firewall usergroup to authenticate clients.	
broadcast-ssid	Enable/disable broadcasting the SSID (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable broadcasting the SSID.	
	<i>disable</i>	Disable broadcasting the SSID.	
broadcast-suppression	Optional suppression of broadcast messages. For example, you can keep DHCP messages, ARP broadcasts, and so on off of the wireless network.	option	-

Parameter	Description	Type	Size

Option	Description
<i>dhcp-up</i>	Suppress broadcast uplink DHCP messages.
<i>dhcp-down</i>	Suppress broadcast downlink DHCP messages.
<i>dhcp-starvation</i>	Suppress broadcast DHCP starvation req messages.
<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.
<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.
<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.
<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.
<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.
<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.
<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.
<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.
<i>ipv6</i>	Suppress IPv6 packets.
<i>all-other-mc</i>	Suppress all other multicast messages.
<i>all-other-bc</i>	Suppress all other broadcast messages.

captive-portal-ac-name	Local-bridging captive portal ac-name.	string	Maximum length: 35
captive-portal-macauth-radius-secret	Secret key to access the macauth RADIUS server.	password	Not Specified
captive-portal-macauth-radius-server	Captive portal external 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-radius-server	Captive portal RADIUS server domain name or IP address.	string	Maximum length: 63
captive-portal-session-timeout-interval	Session timeout interval (0 - 864000 sec, default = 0).	integer	Minimum value: 0 Maximum value: 864000

Parameter	Description	Type	Size
dhcp-lease-time	DHCP lease time in seconds for NAT IP address.	integer	Minimum value: 300 Maximum value: 8640000
dhcp-option82-circuit-id-insertion	Enable/disable DHCP option 82 circuit-id insert (default = disable).	option	-

Option	Description
<i>style-1</i>	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".
<i>style-2</i>	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".
<i>disable</i>	Disable DHCP option 82 circuit-id insert.

dhcp-option82-insertion	Enable/disable DHCP option 82 insert (default = disable).	option	-

Option	Description
<i>enable</i>	Enable DHCP option 82 insert.
<i>disable</i>	Disable DHCP option 82 insert.

dhcp-option82-remote-id-insertion	Enable/disable DHCP option 82 remote-id insert (default = disable).	option	-

Option	Description
<i>style-1</i>	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.
<i>disable</i>	Disable DHCP option 82 remote-id insert.

dynamic-vlan	Enable/disable dynamic VLAN assignment.	option	-

Option	Description
<i>enable</i>	Enable dynamic VLAN assignment.
<i>disable</i>	Disable dynamic VLAN assignment.

eap-reauth	Enable/disable EAP re-authentication for WPA-Enterprise security.	option	-

Option	Description
<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.

Parameter	Description	Type	Size

Option		Description
<i>disable</i>		Disable EAP re-authentication for WPA-Enterprise security.

eap-reauth-intv	EAP re-authentication interval (1800 - 864000 sec, default = 86400).	integer	Minimum value: 1800 Maximum value: 864000

eapol-key-retries	Enable/disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2) (default = enable).	option	-

Option		Description
<i>disable</i>		Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).
<i>enable</i>		Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).

encrypt	Encryption protocol to use (only available when security is set to a WPA type).	option	-

Option		Description
<i>TKIP</i>		Use TKIP encryption.
<i>AES</i>		Use AES encryption.
<i>TKIP-AES</i>		Use TKIP and AES encryption.

external-fast-roaming	Enable/disable fast roaming or pre-authentication with external APs not managed by the FortiGate (default = disable).	option	-

Option		Description
<i>enable</i>		Enable fast roaming or pre-authentication with external APs.
<i>disable</i>		Disable fast roaming or pre-authentication with external APs.

external-logout	URL of external authentication logout server.	string	Maximum length: 127

external-web	URL of external authentication web server.	string	Maximum length: 127

external-web-format	URL query parameter detection (default = auto-detect).	option	-

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-detect</i></td><td>Automatically detect if "external-web" URL has any query parameter.</td></tr><tr><td><i>no-query-string</i></td><td>"external-web" URL does not have any query parameter.</td></tr><tr><td><i>partial-query-string</i></td><td>"external-web" URL has some query parameters.</td></tr></table>	Option	Description	<i>auto-detect</i>	Automatically detect if "external-web" URL has any query parameter.	<i>no-query-string</i>	"external-web" URL does not have any query parameter.	<i>partial-query-string</i>	"external-web" URL has some query parameters.		
Option	Description										
<i>auto-detect</i>	Automatically detect if "external-web" URL has any query parameter.										
<i>no-query-string</i>	"external-web" URL does not have any query parameter.										
<i>partial-query-string</i>	"external-web" URL has some query parameters.										
fast-bss-transition	Enable/disable 802.11r Fast BSS Transition (FT) (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable 802.11r Fast BSS Transition (FT).</td></tr><tr><td><i>enable</i></td><td>Enable 802.11r Fast BSS Transition (FT).</td></tr></table>	Option	Description	<i>disable</i>	Disable 802.11r Fast BSS Transition (FT).	<i>enable</i>	Enable 802.11r Fast BSS Transition (FT).				
Option	Description										
<i>disable</i>	Disable 802.11r Fast BSS Transition (FT).										
<i>enable</i>	Enable 802.11r Fast BSS Transition (FT).										
fast-roaming	Enable/disable fast-roaming, or pre-authentication, where supported by clients (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fast-roaming, or pre-authentication.</td></tr><tr><td><i>disable</i></td><td>Disable fast-roaming, or pre-authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable fast-roaming, or pre-authentication.	<i>disable</i>	Disable fast-roaming, or pre-authentication.				
Option	Description										
<i>enable</i>	Enable fast-roaming, or pre-authentication.										
<i>disable</i>	Disable fast-roaming, or pre-authentication.										
ft-mobility-domain	Mobility domain identifier in FT (1 - 65535, default = 1000).	integer	Minimum value: 1 Maximum value: 65535								
ft-over-ds	Enable/disable FT over the Distribution System (DS).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FT over the Distribution System (DS).</td></tr><tr><td><i>enable</i></td><td>Enable FT over the Distribution System (DS).</td></tr></table>	Option	Description	<i>disable</i>	Disable FT over the Distribution System (DS).	<i>enable</i>	Enable FT over the Distribution System (DS).				
Option	Description										
<i>disable</i>	Disable FT over the Distribution System (DS).										
<i>enable</i>	Enable FT over the Distribution System (DS).										
ft-r0-key-lifetime	Lifetime of the PMK-R0 key in FT, 1-65535 minutes.	integer	Minimum value: 1 Maximum value: 65535								
gtk-rekey	Enable/disable GTK rekey for WPA security.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTK rekey for WPA security.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTK rekey for WPA security.						
Option	Description										
<i>enable</i>	Enable GTK rekey for WPA security.										

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable GTK rekey for WPA security.</td></tr></table>	Option	Description	<i>disable</i>	Disable GTK rekey for WPA security.								
Option	Description												
<i>disable</i>	Disable GTK rekey for WPA security.												
gtk-rekey-intv	GTK rekey interval (1800 - 864000 sec, default = 86400).	integer	Minimum value: 1800 Maximum value: 864000										
high-efficiency	Enable/disable 802.11ax high efficiency (default = enable).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11ax high efficiency.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11ax high efficiency.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11ax high efficiency.	<i>disable</i>	Disable 802.11ax high efficiency.						
Option	Description												
<i>enable</i>	Enable 802.11ax high efficiency.												
<i>disable</i>	Disable 802.11ax high efficiency.												
hotspot20-profile	Hotspot 2.0 profile name.	string	Maximum length: 35										
intra-vap-privacy	Enable/disable blocking communication between clients on the same SSID (called intra-SSID privacy) (default = disable).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intra-SSID privacy.</td></tr><tr><td><i>disable</i></td><td>Disable intra-SSID privacy.</td></tr></table>	Option	Description	<i>enable</i>	Enable intra-SSID privacy.	<i>disable</i>	Disable intra-SSID privacy.						
Option	Description												
<i>enable</i>	Enable intra-SSID privacy.												
<i>disable</i>	Disable intra-SSID privacy.												
ip	IP address and subnet mask for the local standalone NAT subnet.	ipv4-classnet-host	Not Specified										
key	WEP Key.	password	Not Specified										
keyindex	WEP key index (1 - 4).	integer	Minimum value: 1 Maximum value: 4										
ldpc	VAP low-density parity-check (LDPC) coding configuration.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable LDPC.</td></tr><tr><td><i>rx</i></td><td>Enable LDPC when receiving traffic.</td></tr><tr><td><i>tx</i></td><td>Enable LDPC when transmitting traffic.</td></tr><tr><td><i>rxtx</i></td><td>Enable LDPC when both receiving and transmitting traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable LDPC.	<i>rx</i>	Enable LDPC when receiving traffic.	<i>tx</i>	Enable LDPC when transmitting traffic.	<i>rxtx</i>	Enable LDPC when both receiving and transmitting traffic.		
Option	Description												
<i>disable</i>	Disable LDPC.												
<i>rx</i>	Enable LDPC when receiving traffic.												
<i>tx</i>	Enable LDPC when transmitting traffic.												
<i>rxtx</i>	Enable LDPC when both receiving and transmitting traffic.												

Parameter	Description	Type	Size						
local-authentication	Enable/disable AP local authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP local authentication.</td></tr><tr><td><i>disable</i></td><td>Disable AP local authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP local authentication.	<i>disable</i>	Disable AP local authentication.		
Option	Description								
<i>enable</i>	Enable AP local authentication.								
<i>disable</i>	Disable AP local authentication.								
local-bridging	Enable/disable bridging of wireless and Ethernet interfaces on the FortiAP (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP local VAP to Ethernet bridging.</td></tr><tr><td><i>disable</i></td><td>Disable AP local VAP to Ethernet bridging.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP local VAP to Ethernet bridging.	<i>disable</i>	Disable AP local VAP to Ethernet bridging.		
Option	Description								
<i>enable</i>	Enable AP local VAP to Ethernet bridging.								
<i>disable</i>	Disable AP local VAP to Ethernet bridging.								
local-lan	Allow/deny traffic destined for a Class A, B, or C private IP address (default = allow).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow traffic destined for a Class A, B, or C private IP address.</td></tr><tr><td><i>deny</i></td><td>Deny traffic destined for a Class A, B, or C private IP address.</td></tr></table>	Option	Description	<i>allow</i>	Allow traffic destined for a Class A, B, or C private IP address.	<i>deny</i>	Deny traffic destined for a Class A, B, or C private IP address.		
Option	Description								
<i>allow</i>	Allow traffic destined for a Class A, B, or C private IP address.								
<i>deny</i>	Deny traffic destined for a Class A, B, or C private IP address.								
local-standalone	Enable/disable AP local standalone (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP local standalone.</td></tr><tr><td><i>disable</i></td><td>Disable AP local standalone.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP local standalone.	<i>disable</i>	Disable AP local standalone.		
Option	Description								
<i>enable</i>	Enable AP local standalone.								
<i>disable</i>	Disable AP local standalone.								
local-standalone-nat	Enable/disable AP local standalone NAT mode.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP local standalone NAT mode.</td></tr><tr><td><i>disable</i></td><td>Disable AP local standalone NAT mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP local standalone NAT mode.	<i>disable</i>	Disable AP local standalone NAT mode.		
Option	Description								
<i>enable</i>	Enable AP local standalone NAT mode.								
<i>disable</i>	Disable AP local standalone NAT mode.								
mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC authentication bypass.</td></tr><tr><td><i>disable</i></td><td>Disable MAC authentication bypass.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC authentication bypass.	<i>disable</i>	Disable MAC authentication bypass.		
Option	Description								
<i>enable</i>	Enable MAC authentication bypass.								
<i>disable</i>	Disable MAC authentication bypass.								

Parameter	Description	Type	Size						
mac-filter	Enable/disable MAC filtering to block wireless clients by mac address.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC filtering.</td></tr><tr><td><i>disable</i></td><td>Disable MAC filtering.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC filtering.	<i>disable</i>	Disable MAC filtering.		
Option	Description								
<i>enable</i>	Enable MAC filtering.								
<i>disable</i>	Disable MAC filtering.								
mac-filter-policy-other	Allow or block clients with MAC addresses that are not in the filter list.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow clients with MAC addresses that are not in the filter list.</td></tr><tr><td><i>deny</i></td><td>Block clients with MAC addresses that are not in the filter list.</td></tr></table>	Option	Description	<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.	<i>deny</i>	Block clients with MAC addresses that are not in the filter list.		
Option	Description								
<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.								
<i>deny</i>	Block clients with MAC addresses that are not in the filter list.								
max-clients	Maximum number of clients that can connect simultaneously to the VAP (default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 4294967295						
max-clients-ap	Maximum number of clients that can connect simultaneously to the VAP per AP radio (default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 4294967295						
me-disable-thresh	Disable multicast enhancement when this many clients are receiving multicast traffic.	integer	Minimum value: 2 Maximum value: 256						
mesh-backhaul *	Enable/disable using this VAP as a WiFi mesh backhaul (default = disable). This entry is only available when security is set to a WPA type or open.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mesh backhaul.</td></tr><tr><td><i>disable</i></td><td>Disable mesh backhaul.</td></tr></table>	Option	Description	<i>enable</i>	Enable mesh backhaul.	<i>disable</i>	Disable mesh backhaul.		
Option	Description								
<i>enable</i>	Enable mesh backhaul.								
<i>disable</i>	Disable mesh backhaul.								
mpsk	Enable/disable multiple PSK authentication.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multiple PSK authentication</td></tr></table>	Option	Description	<i>enable</i>	Enable multiple PSK authentication				
Option	Description								
<i>enable</i>	Enable multiple PSK authentication								

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable multiple PSK authentication	
mipsk-concurrent-clients	Maximum number of concurrent clients that connect using the same passphrase in multiple PSK authentication (0 - 65535, default = 0, meaning no limitation).	integer	Minimum value: 0 Maximum value: 65535
mu-mimo	Enable/disable Multi-user MIMO (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable Multi-user MIMO.	
	<i>disable</i>	Disable Multi-user MIMO.	
multicast-enhance	Enable/disable converting multicast to unicast to improve performance (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable multicast enhancement.	
	<i>disable</i>	Disable multicast enhancement.	
multicast-rate	Multicast rate (0, 6000, 12000, or 24000 kbps, default = 0).	option	-
	Option	Description	
	<i>0</i>	Use the default multicast rate.	
	<i>6000</i>	6 Mbps.	
	<i>12000</i>	12 Mbps.	
	<i>24000</i>	24 Mbps.	
name	Virtual AP name.	string	Maximum length: 15
okc	Enable/disable Opportunistic Key Caching (OKC) (default = enable).	option	-
	Option	Description	
	<i>disable</i>	Disable Opportunistic Key Caching (OKC).	
	<i>enable</i>	Enable Opportunistic Key Caching (OKC).	
owe-groups	OWE-Groups.	option	-

Parameter	Description	Type	Size

Option	Description
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.

owe-transition	Enable/disable OWE transition mode support.	option	-

Option	Description
<i>disable</i>	Disable OWE transition mode support.
<i>enable</i>	Enable OWE transition mode support.

owe-transition-ssid	OWE transition mode peer SSID.	string	Maximum length: 32
passphrase	WPA pre-shared key (PSK) to be used to authenticate WiFi users.	password	Not Specified
pmf	Protected Management Frames (PMF) support (default = disable).	option	-

Option	Description
<i>disable</i>	Disable PMF completely.
<i>enable</i>	Enable PMF but deny clients without PMF.
<i>optional</i>	Enable PMF and allow clients without PMF.

pmf-assoc-comeback-timeout	Protected Management Frames (PMF) comeback maximum timeout (1-20 sec).	integer	Minimum value: 1 Maximum value: 20
pmf-sa-query-retry-timeout	Protected Management Frames (PMF) SA query retry timeout interval (1 - 5 100s of msec).	integer	Minimum value: 1 Maximum value: 5
port-macauth	Enable/disable LAN port MAC authentication (default = disable).	option	-

Option	Description
<i>disable</i>	Disable LAN port MAC authentication.
<i>radius</i>	Enable LAN port RADIUS-based MAC authentication.
<i>address-group</i>	Enable LAN port address-group based MAC authentication.

Parameter	Description	Type	Size
port-macauth-reauth-timeout	LAN port MAC authentication re-authentication timeout value (default = 7200 sec).	integer	Minimum value: 120 Maximum value: 65535
port-macauth-timeout	LAN port MAC authentication idle timeout value (default = 600 sec).	integer	Minimum value: 60 Maximum value: 65535
portal-message-override-group	Replacement message group for this VAP (only available when security is set to a captive portal type).	string	Maximum length: 35
portal-type	Captive portal functionality. Configure how the captive portal authenticates users and whether it includes a disclaimer.	option	-

Option	Description
<i>auth</i>	Portal for authentication.
<i>auth+disclaimer</i>	Portal for authentication and disclaimer.
<i>disclaimer</i>	Portal for disclaimer.
<i>email-collect</i>	Portal for email collection.
<i>cmcc</i>	Portal for CMCC.
<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.
<i>auth-mac</i>	Portal for authentication and MAC authentication.
<i>external-auth</i>	Portal for external portal authentication.

primary-wag-profile	Primary wireless access gateway profile name.	string	Maximum length: 35

probe-resp-suppression	Enable/disable probe response suppression (to ignore weak signals) (default = disable).	option	-

Option	Description
<i>enable</i>	Enable probe response suppression.
<i>disable</i>	Disable probe response suppression.

probe-resp-threshold	Minimum signal level/threshold in dBm required for the AP response to probe requests (-95 to -20, default = -80).	string	Maximum length: 7

ptk-rekey	Enable/disable PTK rekey for WPA-Enterprise security.	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PTK rekey for WPA-Enterprise security.</td></tr><tr><td><i>disable</i></td><td>Disable PTK rekey for WPA-Enterprise security.</td></tr></table>	Option	Description	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.	<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.		
	Option	Description							
	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.							
<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.								
ptk-rekey-intv	PTK rekey interval (1800 - 864000 sec, default = 86400).	integer	Minimum value: 1800 Maximum value: 864000						
qos-profile	Quality of service profile name.	string	Maximum length: 35						
quarantine	Enable/disable station quarantine (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable station quarantine.</td></tr><tr><td><i>disable</i></td><td>Disable station quarantine.</td></tr></table>	Option	Description	<i>enable</i>	Enable station quarantine.	<i>disable</i>	Disable station quarantine.		
	Option	Description							
	<i>enable</i>	Enable station quarantine.							
<i>disable</i>	Disable station quarantine.								
radio-2g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 2.4G band (-95 to -20, default = -79).	string	Maximum length: 7						
radio-5g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 5G band(-95 to -20, default = -76).	string	Maximum length: 7						
radio-sensitivity	Enable/disable software radio sensitivity (to ignore weak signals) (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable software radio sensitivity.</td></tr><tr><td><i>disable</i></td><td>Disable software radio sensitivity.</td></tr></table>	Option	Description	<i>enable</i>	Enable software radio sensitivity.	<i>disable</i>	Disable software radio sensitivity.		
	Option	Description							
	<i>enable</i>	Enable software radio sensitivity.							
<i>disable</i>	Disable software radio sensitivity.								
radius-mac-auth	Enable/disable RADIUS-based MAC authentication of clients (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS-based MAC authentication.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS-based MAC authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS-based MAC authentication.	<i>disable</i>	Disable RADIUS-based MAC authentication.		
	Option	Description							
	<i>enable</i>	Enable RADIUS-based MAC authentication.							
<i>disable</i>	Disable RADIUS-based MAC authentication.								
radius-mac-auth-server	RADIUS-based MAC authentication server.	string	Maximum length: 35						

Parameter	Description	Type	Size
radius-mac-auth-usergroups <name>	Selective user groups that are permitted for RADIUS mac authentication. User group name.	string	Maximum length: 79
radius-server	RADIUS server to be used to authenticate WiFi users.	string	Maximum length: 35
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.
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.

Parameter	Description	Type	Size
rates-11ac-ss12	Allowed data rates for 802.11ac/ax with 1 or 2 spatial streams.	option	-
	Option	Description	
	<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.	
	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.	
	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.	
	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.	
	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.	
	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.	
	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.	
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.	
	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.	
	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.	
	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.	
	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.	
	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.	
	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.	
	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.	
	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.	
	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.	
	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.	
	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.	
	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.	
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	
	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	
<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.		
<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.		
rates-11ac-ss34	Allowed data rates for 802.11ac/ax with 3 or 4 spatial streams.	option	-

Parameter	Description	Type	Size

Option	Description
<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.
<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.
<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.
<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.
<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.
<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.
<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.
<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.
<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.
<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.
<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.
<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.
<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.
<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.
<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.
<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.
<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.
<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.
<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.
<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.
<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.
<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.
<i>mcs10/4</i>	Data rate for MCS index 10 with 4 spatial streams.
<i>mcs11/4</i>	Data rate for MCS index 11 with 4 spatial streams.

rates-11bg	Allowed data rates for 802.11b/g.	option	-

Option	Description
1	1 Mbps supported rate.
1-basic	1 Mbps BSS basic rate.

Parameter	Description	Type	Size

Option	Description
2	2 Mbps supported rate.
2-basic	2 Mbps BSS basic rate.
5.5	5.5 Mbps supported rate.
5.5-basic	5.5 Mbps BSS basic rate.
11	11 Mbps supported rate.
11-basic	11 Mbps BSS basic rate.
6	6 Mbps supported rate.
6-basic	6 Mbps BSS basic rate.
9	9 Mbps supported rate.
9-basic	9 Mbps BSS basic rate.
12	12 Mbps supported rate.
12-basic	12 Mbps BSS basic rate.
18	18 Mbps supported rate.
18-basic	18 Mbps BSS basic rate.
24	24 Mbps supported rate.
24-basic	24 Mbps BSS basic rate.
36	36 Mbps supported rate.
36-basic	36 Mbps BSS basic rate.
48	48 Mbps supported rate.
48-basic	48 Mbps BSS basic rate.
54	54 Mbps supported rate.
54-basic	54 Mbps BSS basic rate.

rates-11n-ss12	Allowed data rates for 802.11n with 1 or 2 spatial streams.	option	-

Option	Description
mcs0/1	Data rate for MCS index 0 with 1 spatial stream.
mcs1/1	Data rate for MCS index 1 with 1 spatial stream.
mcs2/1	Data rate for MCS index 2 with 1 spatial stream.

Parameter	Description	Type	Size
	Option	Description	
	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.	
	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.	
	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.	
	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.	
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.	
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	
	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	
	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.	
	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.	
	<i>mcs12/2</i>	Data rate for MCS index 12 with 2 spatial streams.	
	<i>mcs13/2</i>	Data rate for MCS index 13 with 2 spatial streams.	
	<i>mcs14/2</i>	Data rate for MCS index 14 with 2 spatial streams.	
<i>mcs15/2</i>	Data rate for MCS index 15 with 2 spatial streams.		

rates-11n-ss34 Allowed data rates for 802.11n with 3 or 4 spatial streams. option -

Option	Description
<i>mcs16/3</i>	Data rate for MCS index 16 with 3 spatial streams.
<i>mcs17/3</i>	Data rate for MCS index 17 with 3 spatial streams.
<i>mcs18/3</i>	Data rate for MCS index 18 with 3 spatial streams.
<i>mcs19/3</i>	Data rate for MCS index 19 with 3 spatial streams.
<i>mcs20/3</i>	Data rate for MCS index 20 with 3 spatial streams.
<i>mcs21/3</i>	Data rate for MCS index 21 with 3 spatial streams.
<i>mcs22/3</i>	Data rate for MCS index 22 with 3 spatial streams.
<i>mcs23/3</i>	Data rate for MCS index 23 with 3 spatial streams.
<i>mcs24/4</i>	Data rate for MCS index 24 with 4 spatial streams.
<i>mcs25/4</i>	Data rate for MCS index 25 with 4 spatial streams.
<i>mcs26/4</i>	Data rate for MCS index 26 with 4 spatial streams.
<i>mcs27/4</i>	Data rate for MCS index 27 with 4 spatial streams.

Parameter	Description	Type	Size																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs28/4</i></td><td>Data rate for MCS index 28 with 4 spatial streams.</td></tr><tr><td><i>mcs29/4</i></td><td>Data rate for MCS index 29 with 4 spatial streams.</td></tr><tr><td><i>mcs30/4</i></td><td>Data rate for MCS index 30 with 4 spatial streams.</td></tr><tr><td><i>mcs31/4</i></td><td>Data rate for MCS index 31 with 4 spatial streams.</td></tr></table>	Option	Description	<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.	<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.	<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.	<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.										
	Option	Description																			
	<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.																			
	<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.																			
	<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.																			
<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.																				
sae-groups	SAE-Groups.	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr></table>	Option	Description	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.												
	Option	Description																			
	19	DH Group 19.																			
	20	DH Group 20.																			
21	DH Group 21.																				
sae-password	WPA3 SAE password to be used to authenticate WiFi users.	password	Not Specified																		
schedule <name>	Firewall schedules for enabling this VAP on the FortiAP. This VAP will be enabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35																		
secondary-wag-profile	Secondary wireless access gateway profile name.	string	Maximum length: 35																		
security	Security mode for the wireless interface (default = wpa2-only-personal).	option	-																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>captive-portal</i></td><td>Captive portal.</td></tr><tr><td><i>wep64</i></td><td>WEP 64-bit.</td></tr><tr><td><i>wep128</i></td><td>WEP 128-bit.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-personal+captive-portal</i></td><td>WPA/WPA2 personal with captive portal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr><tr><td><i>wpa-only-personal</i></td><td>WPA personal.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>captive-portal</i>	Captive portal.	<i>wep64</i>	WEP 64-bit.	<i>wep128</i>	WEP 128-bit.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.	<i>wpa-only-personal</i>	WPA personal.		
	Option	Description																			
	<i>open</i>	Open.																			
	<i>captive-portal</i>	Captive portal.																			
	<i>wep64</i>	WEP 64-bit.																			
	<i>wep128</i>	WEP 128-bit.																			
	<i>wpa-personal</i>	WPA/WPA2 personal.																			
	<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.																			
	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.																			
<i>wpa-only-personal</i>	WPA personal.																				

Parameter	Description	Type	Size

Option	Description
<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.
<i>wpa-only-enterprise</i>	WPA enterprise.
<i>wpa2-only-personal</i>	WPA2 personal.
<i>wpa2-only-personal+captive-portal</i>	WPA2 personal with captive portal.
<i>wpa2-only-enterprise</i>	WPA2 enterprise.
<i>wpa3-enterprise</i>	WPA3 enterprise.
<i>wpa3-sae</i>	WPA3 SAE.
<i>wpa3-sae-transition</i>	WPA3 SAE transition.
<i>owe</i>	Opportunistic wireless encryption.
<i>osen</i>	OSEN.

security-exempt-list	Optional security exempt list for captive portal authentication.	string	Maximum length: 35
security-redirect-url	Optional URL for redirecting users after they pass captive portal authentication.	string	Maximum length: 127
selected-usergroups <name>	Selective user groups that are permitted to authenticate. User group name.	string	Maximum length: 79
split-tunneling	Enable/disable split tunneling (default = disable).	option	-

Option	Description
<i>enable</i>	Enable split tunneling.
<i>disable</i>	Disable split tunneling.

ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string	Maximum length: 32
target-wake-time	Enable/disable 802.11ax target wake time (default = enable).	option	-

Parameter	Description	Type	Size
	Option	Description	
	enable	Enable 802.11ax target wake time.	
	disable	Disable 802.11ax target wake time.	
tkip-counter-measure	Enable/disable TKIP counter measure.	option	-
	Option	Description	
	enable	Enable TKIP counter measure.	
	disable	Disable TKIP counter measure.	
tunnel-echo-interval	The time interval to send echo to both primary and secondary tunnel peers (1 - 65535 sec, default = 300).	integer	Minimum value: 1 Maximum value: 65535
tunnel-fallback-interval	The time interval for secondary tunnel to fall back to primary tunnel (0 - 65535 sec, default = 7200).	integer	Minimum value: 0 Maximum value: 65535
usergroup <name>	Firewall user group to be used to authenticate WiFi users. User group name.	string	Maximum length: 79
utm-profile	UTM profile name.	string	Maximum length: 35
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.	
vlan-pooling	Enable/disable VLAN pooling, to allow grouping of multiple wireless controller VLANs into VLAN pools (default = disable). When set to wtp-group, VLAN pooling occurs with VLAN assignment by wtp-group.	option	-
	Option	Description	
	wtp-group	Enable VLAN pooling with VLAN assignment by wtp-group.	

Parameter	Description	Type	Size
	Option	Description	
	<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.	
	<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.	
	<i>disable</i>	Disable VLAN pooling.	
vlanid	Optional VLAN ID.	integer	Minimum value: 0 Maximum value: 4094
voice-enterprise	Enable/disable 802.11k and 802.11v assisted Voice-Enterprise roaming (default = disable).	option	-
	Option	Description	
	<i>disable</i>	Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.	
	<i>enable</i>	Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.	

* This parameter may not exist in some models.

config mac-filter-list

Parameter	Description	Type	Size						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295						
mac	MAC address.	mac-address	Not Specified						
mac-filter-policy	Deny or allow the client with this MAC address.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the client with this MAC address.</td></tr><tr><td><i>deny</i></td><td>Block the client with this MAC address.</td></tr></table>			Option	Description	<i>allow</i>	Allow the client with this MAC address.	<i>deny</i>	Block the client with this MAC address.
Option	Description								
<i>allow</i>	Allow the client with this MAC address.								
<i>deny</i>	Block the client with this MAC address.								

config mpsk-key

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

Parameter	Description	Type	Size
concurrent-clients	Number of clients that can connect using this pre-shared key.	string	Maximum length: 15
key-name	Pre-shared key name.	string	Maximum length: 35
mpsk-schedules <name>	Firewall schedule for MPSPK passphrase. The passphrase will be effective only when at least one schedule is valid. Schedule name.	string	Maximum length: 35
passphrase	WPA Pre-shared key.	password	Not Specified

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-login-failed-page	Override auth-login-failed-page message with message from portal-message-overrides group.	string	Maximum length: 35
auth-login-page	Override auth-login-page message with message from portal-message-overrides group.	string	Maximum length: 35
auth-reject-page	Override auth-reject-page message with message from portal-message-overrides group.	string	Maximum length: 35

config vlan-pool

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4094
wtp-group	WTP group name.	string	Maximum length: 35

config wireless-controller vap-group

Configure virtual Access Point (VAP) groups.

```
config wireless-controller vap-group
    Description: Configure virtual Access Point (VAP) groups.
    edit <name>
        set comment {var-string}
```

```

        set vaps <name1>, <name2>, ...
    next
end

```

config wireless-controller vap-group

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
name	Group Name	string	Maximum length: 35
vaps <name>	List of SSIDs to be included in the VAP group. vap name	string	Maximum length: 35

config wireless-controller wag-profile

Configure wireless access gateway (WAG) profiles used for tunnels on AP.

```

config wireless-controller wag-profile
    Description: Configure wireless access gateway (WAG) profiles used for tunnels on AP.
    edit <name>
        set comment {var-string}
        set dhcp-ip-addr {ipv4-address}
        set ping-interval {integer}
        set ping-number {integer}
        set return-packet-timeout {integer}
        set tunnel-type [l2tpv3|gre]
        set wag-ip {ipv4-address}
        set wag-port {integer}
    next
end

```

config wireless-controller wag-profile

Parameter	Description	Type	Size
comment	Comment.	var-string	Maximum length: 255
dhcp-ip-addr	IP address of the monitoring DHCP request packet sent through the tunnel.	ipv4-address	Not Specified
name	Tunnel profile name.	string	Maximum length: 35

Parameter	Description	Type	Size						
ping-interval	Interval between two tunnel monitoring echo packets (1 - 65535 sec, default = 1).	integer	Minimum value: 1 Maximum value: 65535						
ping-number	Number of the tunnel monitoring echo packets (1 - 65535, default = 5).	integer	Minimum value: 1 Maximum value: 65535						
return-packet-timeout	Window of time for the return packets from the tunnel's remote end (1 - 65535 sec, default = 160).	integer	Minimum value: 1 Maximum value: 65535						
tunnel-type	Tunnel type.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>l2tpv3</i></td><td>L2TPv3 Ethernet Pseudowire.</td></tr><tr><td><i>gre</i></td><td>GRE Ethernet tunnel.</td></tr></table>			Option	Description	<i>l2tpv3</i>	L2TPv3 Ethernet Pseudowire.	<i>gre</i>	GRE Ethernet tunnel.
Option	Description								
<i>l2tpv3</i>	L2TPv3 Ethernet Pseudowire.								
<i>gre</i>	GRE Ethernet tunnel.								
wag-ip	IP Address of the wireless access gateway.	ipv4-address	Not Specified						
wag-port	UDP port of the wireless access gateway.	integer	Minimum value: 0 Maximum value: 65535						

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 ap-auto-suppress [enable|disable]
    set ap-bgscan-disable-schedules <name1>, <name2>, ...
    set ap-bgscan-duration {integer}
    set ap-bgscan-idle {integer}
    set ap-bgscan-intv {integer}
    set ap-bgscan-period {integer}
    set ap-bgscan-report-intv {integer}
    set ap-fgscan-report-intv {integer}
    set ap-scan [disable|enable]
    set ap-scan-passive [enable|disable]
    set ap-scan-threshold {string}
    set asleap-attack [enable|disable]
    set assoc-flood-thresh {integer}
```

```

set assoc-flood-time {integer}
set assoc-frame-flood [enable|disable]
set auth-flood-thresh {integer}
set auth-flood-time {integer}
set auth-frame-flood [enable|disable]
set comment {string}
set deauth-broadcast [enable|disable]
set deauth-unknown-src-thresh {integer}
set eapol-fail-flood [enable|disable]
set eapol-fail-intv {integer}
set eapol-fail-thresh {integer}
set eapol-logoff-flood [enable|disable]
set eapol-logoff-intv {integer}
set eapol-logoff-thresh {integer}
set eapol-pre-fail-flood [enable|disable]
set eapol-pre-fail-intv {integer}
set eapol-pre-fail-thresh {integer}
set eapol-pre-succ-flood [enable|disable]
set eapol-pre-succ-intv {integer}
set eapol-pre-succ-thresh {integer}
set eapol-start-flood [enable|disable]
set eapol-start-intv {integer}
set eapol-start-thresh {integer}
set eapol-succ-flood [enable|disable]
set eapol-succ-intv {integer}
set eapol-succ-thresh {integer}
set invalid-mac-oui [enable|disable]
set long-duration-attack [enable|disable]
set long-duration-thresh {integer}
set null-ssid-probe-resp [enable|disable]
set sensor-mode [disable|foreign|...]
set spoofed-deauth [enable|disable]
set weak-wep-iv [enable|disable]
set wireless-bridge [enable|disable]

```

next

end

config wireless-controller wids-profile

Parameter	Description	Type	Size						
ap-auto-suppress	Enable/disable on-wire rogue AP auto-suppression (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable on-wire rogue AP auto-suppression.</td></tr><tr><td><i>disable</i></td><td>Disable on-wire rogue AP auto-suppression.</td></tr></table>			Option	Description	<i>enable</i>	Enable on-wire rogue AP auto-suppression.	<i>disable</i>	Disable on-wire rogue AP auto-suppression.
	Option	Description							
	<i>enable</i>	Enable on-wire rogue AP auto-suppression.							
<i>disable</i>	Disable on-wire rogue AP auto-suppression.								
ap-bgscan-disable-schedules <name>	Firewall schedules for turning off FortiAP radio background scan. Background scan will be disabled when at least one of the schedules is valid. Separate multiple schedule names with a space.	string	Maximum length: 35						

Parameter	Description	Type	Size						
	Schedule name.								
ap-bgscan-duration	Listening time on a scanning channel (10 - 1000 msec, default = 20).	integer	Minimum value: 10 Maximum value: 1000						
ap-bgscan-idle	Waiting time for channel inactivity before scanning this channel (0 - 1000 msec, default = 0).	integer	Minimum value: 0 Maximum value: 1000						
ap-bgscan-intv	Period of time between scanning two channels (1 - 600 sec, default = 1).	integer	Minimum value: 1 Maximum value: 600						
ap-bgscan-period	Period of time between background scans (60 - 3600 sec, default = 600).	integer	Minimum value: 60 Maximum value: 3600						
ap-bgscan-report-intv	Period of time between background scan reports (15 - 600 sec, default = 30).	integer	Minimum value: 15 Maximum value: 600						
ap-fgscan-report-intv	Period of time between foreground scan reports (15 - 600 sec, default = 15).	integer	Minimum value: 15 Maximum value: 600						
ap-scan	Enable/disable rogue AP detection.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable rogue AP detection.</td></tr><tr><td>enable</td><td>Enable rogue AP detection.</td></tr></table>	Option	Description	disable	Disable rogue AP detection.	enable	Enable rogue AP detection.		
Option	Description								
disable	Disable rogue AP detection.								
enable	Enable rogue AP detection.								
ap-scan-passive	Enable/disable passive scanning. Enable means do not send probe request on any channels (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Passive scanning on all channels.</td></tr><tr><td>disable</td><td>Passive scanning only on DFS channels.</td></tr></table>	Option	Description	enable	Passive scanning on all channels.	disable	Passive scanning only on DFS channels.		
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 (-95 to -20, default = -90).	string	Maximum length: 7
asleep-attack	Enable/disable asleep attack detection (default = disable).	option	-

Option	Description

<i>enable</i>	Enable asleep attack detection.

<i>disable</i>	Disable asleep attack detection.

assoc-flood-thresh	The threshold value for association frame flooding.	integer	Minimum value: 1 Maximum value: 100
assoc-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120
assoc-frame-flood	Enable/disable association frame flooding detection (default = disable).	option	-

Option	Description

<i>enable</i>	Enable association frame flooding detection.

<i>disable</i>	Disable association frame flooding detection.

auth-flood-thresh	The threshold value for authentication frame flooding.	integer	Minimum value: 1 Maximum value: 100
auth-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120
auth-frame-flood	Enable/disable authentication frame flooding detection (default = disable).	option	-

Option	Description

<i>enable</i>	Enable authentication frame flooding detection.

<i>disable</i>	Disable authentication frame flooding detection.

Parameter	Description	Type	Size						
comment	Comment.	string	Maximum length: 63						
deauth-broadcast	Enable/disable broadcasting de-authentication detection (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast de-authentication detection.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast de-authentication detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast de-authentication detection.	<i>disable</i>	Disable broadcast de-authentication detection.		
Option	Description								
<i>enable</i>	Enable broadcast de-authentication detection.								
<i>disable</i>	Disable broadcast de-authentication detection.								
deauth-unknown-src-thresh	Threshold value per second to deauth unknown src for DoS attack (0: no limit).	integer	Minimum value: 0 Maximum value: 65535						
eapol-fail-flood	Enable/disable EAPOL-Failure flooding (to AP) detection (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Failure flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Failure flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Failure flooding detection.	<i>disable</i>	Disable EAPOL-Failure flooding detection.		
Option	Description								
<i>enable</i>	Enable EAPOL-Failure flooding detection.								
<i>disable</i>	Disable EAPOL-Failure flooding detection.								
eapol-fail-intv	The detection interval for EAPOL-Failure flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600						
eapol-fail-thresh	The threshold value for EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100						
eapol-logoff-flood	Enable/disable EAPOL-Logoff flooding (to AP) detection (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Logoff flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Logoff flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Logoff flooding detection.	<i>disable</i>	Disable EAPOL-Logoff flooding detection.		
Option	Description								
<i>enable</i>	Enable EAPOL-Logoff flooding detection.								
<i>disable</i>	Disable EAPOL-Logoff flooding detection.								
eapol-logoff-intv	The detection interval for EAPOL-Logoff flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600						

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-pre-fail-flood	Enable/disable premature EAPOL-Failure flooding (to STA) detection (default = disable).	option	-

Option	Description

<i>enable</i>	Enable premature EAPOL-Failure flooding detection.
<i>disable</i>	Disable premature EAPOL-Failure flooding detection.

eapol-pre-fail-intv	The detection interval for premature EAPOL-Failure flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600
eapol-pre-fail-thresh	The threshold value for premature EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100
eapol-pre-succ-flood	Enable/disable premature EAPOL-Success flooding (to STA) detection (default = disable).	option	-

Option	Description

<i>enable</i>	Enable premature EAPOL-Success flooding detection.
<i>disable</i>	Disable premature EAPOL-Success flooding detection.

eapol-pre-succ-intv	The detection interval for premature EAPOL-Success flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600
eapol-pre-succ-thresh	The threshold value for premature EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100
eapol-start-flood	Enable/disable EAPOL-Start flooding (to AP) detection (default = disable).	option	-

Option	Description

<i>enable</i>	Enable EAPOL-Start flooding detection.
<i>disable</i>	Disable EAPOL-Start flooding detection.

Parameter	Description	Type	Size						
eapol-start-intv	The detection interval for EAPOL-Start flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600						
eapol-start-thresh	The threshold value for EAPOL-Start flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100						
eapol-succ-flood	Enable/disable EAPOL-Success flooding (to AP) detection (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable EAPOL-Success flooding detection.</td></tr><tr><td>disable</td><td>Disable EAPOL-Success flooding detection.</td></tr></table>	Option	Description	enable	Enable EAPOL-Success flooding detection.	disable	Disable EAPOL-Success flooding detection.		
Option	Description								
enable	Enable EAPOL-Success flooding detection.								
disable	Disable EAPOL-Success flooding detection.								
eapol-succ-intv	The detection interval for EAPOL-Success flooding (1 - 3600 sec).	integer	Minimum value: 1 Maximum value: 3600						
eapol-succ-thresh	The threshold value for EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100						
invalid-mac-oui	Enable/disable invalid MAC OUI detection.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable invalid MAC OUI detection.</td></tr><tr><td>disable</td><td>Disable invalid MAC OUI detection.</td></tr></table>	Option	Description	enable	Enable invalid MAC OUI detection.	disable	Disable invalid MAC OUI detection.		
Option	Description								
enable	Enable invalid MAC OUI detection.								
disable	Disable invalid MAC OUI detection.								
long-duration-attack	Enable/disable long duration attack detection based on user configured threshold (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable long duration attack detection.</td></tr><tr><td>disable</td><td>Disable long duration attack detection.</td></tr></table>	Option	Description	enable	Enable long duration attack detection.	disable	Disable long duration attack detection.		
Option	Description								
enable	Enable long duration attack detection.								
disable	Disable long duration attack detection.								
long-duration-thresh	Threshold value for long duration attack detection (1000 - 32767 usec, default = 8200).	integer	Minimum value: 1000 Maximum value: 32767						

Parameter	Description	Type	Size								
name	WIDS profile name.	string	Maximum length: 35								
null-ssid-probe-resp	Enable/disable null SSID probe response detection (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable null SSID probe resp detection.</td></tr><tr><td><i>disable</i></td><td>Disable null SSID probe resp detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable null SSID probe resp detection.	<i>disable</i>	Disable null SSID probe resp detection.				
Option	Description										
<i>enable</i>	Enable null SSID probe resp detection.										
<i>disable</i>	Disable null SSID probe resp detection.										
sensor-mode	Scan nearby WiFi stations (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the scan.</td></tr><tr><td><i>foreign</i></td><td>Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.</td></tr><tr><td><i>both</i></td><td>Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.</td></tr></table>	Option	Description	<i>disable</i>	Disable the scan.	<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.	<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.		
Option	Description										
<i>disable</i>	Disable the scan.										
<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.										
<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.										
spoofed-deauth	Enable/disable spoofed de-authentication attack detection (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable spoofed de-authentication attack detection.</td></tr><tr><td><i>disable</i></td><td>Disable spoofed de-authentication attack detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable spoofed de-authentication attack detection.	<i>disable</i>	Disable spoofed de-authentication attack detection.				
Option	Description										
<i>enable</i>	Enable spoofed de-authentication attack detection.										
<i>disable</i>	Disable spoofed de-authentication attack detection.										
weak-wep-iv	Enable/disable weak WEP IV (Initialization Vector) detection (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable weak WEP IV detection.</td></tr><tr><td><i>disable</i></td><td>Disable weak WEP IV detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable weak WEP IV detection.	<i>disable</i>	Disable weak WEP IV detection.				
Option	Description										
<i>enable</i>	Enable weak WEP IV detection.										
<i>disable</i>	Disable weak WEP IV detection.										
wireless-bridge	Enable/disable wireless bridge detection (default = disable).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless bridge detection.</td></tr><tr><td><i>disable</i></td><td>Disable wireless bridge detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable wireless bridge detection.	<i>disable</i>	Disable wireless bridge detection.				
Option	Description										
<i>enable</i>	Enable wireless bridge detection.										
<i>disable</i>	Disable wireless bridge detection.										

config wireless-controller wtp

Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate.

```
config wireless-controller wtp
    Description: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to
    be managed by FortiGate.
    edit <wtp-id>
        set admin [discovered|disable|...]
        set allowaccess {option1}, {option2}, ...
        set bonjour-profile {string}
        set coordinate-latitude {string}
        set coordinate-longitude {string}
        set image-download [enable|disable]
        set index {integer}
        set ip-fragment-preventing {option1}, {option2}, ...
        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 led-state [enable|disable]
        set location {string}
        set login-passwd {password}
        set login-passwd-change [yes|default|...]
        set mesh-bridge-enable [default|enable|...]
        set name {string}
        set override-allowaccess [enable|disable]
        set override-ip-fragment [enable|disable]
        set override-lan [enable|disable]
        set override-led-state [enable|disable]
        set override-login-passwd-change [enable|disable]
        set override-split-tunnel [enable|disable]
        set override-wan-port-mode [enable|disable]
        config radio-1
            Description: Configuration options for radio 1.
            set auto-power-high {integer}
            set auto-power-level [enable|disable]
            set auto-power-low {integer}
```

```

    set band [802.11a|802.11b|...]
    set channel <chan1>, <chan2>, ...
    set override-analysis [enable|disable]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}
    set spectrum-analysis [enable|disable]
    set vap-all [enable|disable]
    set vaps <name1>, <name2>, ...
end
config radio-2
    Description: Configuration options for radio 2.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set band [802.11a|802.11b|...]
    set channel <chan1>, <chan2>, ...
    set override-analysis [enable|disable]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}
    set spectrum-analysis [enable|disable]
    set vap-all [enable|disable]
    set vaps <name1>, <name2>, ...
end
config radio-3
    Description: Configuration options for radio 3.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set band [802.11a|802.11b|...]
    set channel <chan1>, <chan2>, ...
    set override-analysis [enable|disable]
    set override-band [enable|disable]
    set override-channel [enable|disable]
    set override-txpower [enable|disable]
    set override-vaps [enable|disable]
    set power-level {integer}
    set spectrum-analysis [enable|disable]
    set vap-all [enable|disable]
    set vaps <name1>, <name2>, ...
end
config radio-4
    Description: Configuration options for radio 4.
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set band [802.11a|802.11b|...]
    set channel <chan1>, <chan2>, ...
    set override-analysis [enable|disable]
    set override-band [enable|disable]
    set override-channel [enable|disable]

```

```

        set override-txpower [enable|disable]
        set override-vaps [enable|disable]
        set power-level {integer}
        set spectrum-analysis [enable|disable]
        set vap-all [enable|disable]
        set vaps <name1>, <name2>, ...
    end
    set region {string}
    set region-x {string}
    set region-y {string}
    config split-tunneling-acl
        Description: Split tunneling ACL filter list.
        edit <id>
            set dest-ip {ipv4-classnet}
        next
    end
    set split-tunneling-acl-local-ap-subnet [enable|disable]
    set split-tunneling-acl-path [tunnel|local]
    set tun-mtu-downlink {integer}
    set tun-mtu-uplink {integer}
    set wan-port-mode [wan-lan|wan-only]
    set wtp-mode [normal|remote]
    set wtp-profile {string}
next
end

```

config wireless-controller wtp

Parameter	Description	Type	Size								
admin	Configure how the FortiGate operating as a wireless controller discovers and manages this WTP, AP or FortiAP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discovered</i></td><td>FortiGate wireless controller discovers the WTP, AP, or FortiAP through discovery or join request messages.</td></tr><tr><td><i>disable</i></td><td>FortiGate wireless controller is configured to not provide service to this WTP.</td></tr><tr><td><i>enable</i></td><td>FortiGate wireless controller is configured to provide service to this WTP.</td></tr></table>	Option	Description	<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP through discovery or join request messages.	<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.	<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.		
Option	Description										
<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP through discovery or join request messages.										
<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.										
<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.										
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.		
Option	Description										
<i>https</i>	HTTPS access.										
<i>ssh</i>	SSH access.										
<i>snmp</i>	SNMP access.										

Parameter	Description	Type	Size
bonjour-profile	Bonjour profile name.	string	Maximum length: 35
coordinate-latitude	WTP latitude coordinate.	string	Maximum length: 19
coordinate-longitude	WTP longitude coordinate.	string	Maximum length: 19
image-download	Enable/disable WTP image download.	option	-
	Option	Description	
	<i>enable</i>	Enable WTP image download at join time.	
	<i>disable</i>	Disable WTP image download at join time.	
index	Index (0 - 4294967295). Read-only.	integer	Minimum value: 0 Maximum value: 4294967295
ip-fragment-preventing	Method(s) by which IP fragmentation is prevented for control and data packets through CAPWAP tunnel (default = tcp-mss-adjust).	option	-
	Option	Description	
	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.	
	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable	
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	
	<i>enable</i>	Allow the LEDs on this FortiAP to light.	
	<i>disable</i>	Keep the LEDs on this FortiAP off.	
location	Field for describing the physical location of the WTP, AP or FortiAP.	string	Maximum length: 35
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified

Parameter	Description	Type	Size								
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP (yes, default, or no, default = no).	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>yes</td><td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td></tr><tr><td>default</td><td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td></tr><tr><td>no</td><td>Do not change the managed WTP, FortiAP or AP's administrator password.</td></tr></table>	Option	Description	yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.	default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	no	Do not change the managed WTP, FortiAP or AP's administrator password.		
Option	Description										
yes	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.										
default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.										
no	Do not change the managed WTP, FortiAP or AP's administrator password.										
mesh-bridge-enable	Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Use mesh Ethernet bridge local setting on the WTP.</td></tr><tr><td>enable</td><td>Turn on mesh Ethernet bridge on the WTP.</td></tr><tr><td>disable</td><td>Turn off mesh Ethernet bridge on the WTP.</td></tr></table>	Option	Description	default	Use mesh Ethernet bridge local setting on the WTP.	enable	Turn on mesh Ethernet bridge on the WTP.	disable	Turn off mesh Ethernet bridge on the WTP.		
Option	Description										
default	Use mesh Ethernet bridge local setting on the WTP.										
enable	Turn on mesh Ethernet bridge on the WTP.										
disable	Turn off mesh Ethernet bridge on the WTP.										
name	WTP, AP or FortiAP configuration name.	string	Maximum length: 35								
override-allowaccess	Enable to override the WTP profile management access configuration.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile management access configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile management access configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile management access configuration.	disable	Use the WTP profile management access configuration.				
Option	Description										
enable	Override the WTP profile management access configuration.										
disable	Use the WTP profile management access configuration.										
override-ip-fragment	Enable/disable overriding the WTP profile IP fragment prevention setting.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile IP fragment prevention setting.</td></tr><tr><td>disable</td><td>Use the WTP profile IP fragment prevention setting.</td></tr></table>	Option	Description	enable	Override the WTP profile IP fragment prevention setting.	disable	Use the WTP profile IP fragment prevention setting.				
Option	Description										
enable	Override the WTP profile IP fragment prevention setting.										
disable	Use the WTP profile IP fragment prevention setting.										
override-lan	Enable to override the WTP profile LAN port setting.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile LAN port setting.</td></tr><tr><td>disable</td><td>Use the WTP profile LAN port setting.</td></tr></table>	Option	Description	enable	Override the WTP profile LAN port setting.	disable	Use the WTP profile LAN port setting.				
Option	Description										
enable	Override the WTP profile LAN port setting.										
disable	Use the WTP profile LAN port setting.										

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	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile LED state.</td></tr><tr><td>disable</td><td>Use the WTP profile LED state.</td></tr></table>	Option	Description	enable	Override the WTP profile LED state.	disable	Use the WTP profile LED state.		
Option	Description								
enable	Override the WTP profile LED state.								
disable	Use the WTP profile LED state.								
override-login-passwd-change	Enable to override the WTP profile login-password (administrator password) setting.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile login-password (administrator password)</td></tr><tr><td>disable</td><td>Use the the WTP profile login-password (administrator password)</td></tr></table>	Option	Description	enable	Override the WTP profile login-password (administrator password)	disable	Use the the WTP profile login-password (administrator password)		
Option	Description								
enable	Override the WTP profile login-password (administrator password)								
disable	Use the the WTP profile login-password (administrator password)								
override-split-tunnel	Enable/disable overriding the WTP profile split tunneling setting.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile split tunneling setting.</td></tr><tr><td>disable</td><td>Use the WTP profile split tunneling setting.</td></tr></table>	Option	Description	enable	Override the WTP profile split tunneling setting.	disable	Use the WTP profile split tunneling setting.		
Option	Description								
enable	Override the WTP profile split tunneling setting.								
disable	Use the WTP profile split tunneling setting.								
override-wan-port-mode	Enable/disable overriding the wan-port-mode in the WTP profile.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile wan-port-mode.</td></tr><tr><td>disable</td><td>Use the wan-port-mode in the WTP profile.</td></tr></table>	Option	Description	enable	Override the WTP profile wan-port-mode.	disable	Use the wan-port-mode in the WTP profile.		
Option	Description								
enable	Override the WTP profile wan-port-mode.								
disable	Use the wan-port-mode in the WTP profile.								
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						
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL (default = disable).	option	-						

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.
<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.

split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-

Option	Description
<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.
<i>local</i>	Split tunneling ACL list traffic will be local NATed.

tun-mtu-downlink	The MTU of downlink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 576 Maximum value: 1500
tun-mtu-uplink	The maximum transmission unit (MTU) of uplink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 576 Maximum value: 1500
wan-port-mode	Enable/disable using the FortiAP WAN port as a LAN port.	option	-

Option	Description
<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.
<i>wan-only</i>	Do not use the WAN port as a LAN port.

wtp-id	WTP ID.	string	Maximum length: 35
wtp-mode	WTP, AP, or FortiAP operating mode; normal (by default) 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
<i>normal</i>	Normal WTP, AP, or FortiAP.
<i>remote</i>	Remote WTP, AP, or FortiAP.

Parameter	Description	Type	Size
wtp-profile	WTP profile name to apply to this WTP, AP or FortiAP.	string	Maximum length: 35

config lan

Parameter	Description	Type	Size
port-mode	LAN port mode.	option	-

Option	Description
<i>offline</i>	Offline.
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.

port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15

port1-mode	LAN port 1 mode.	option	-

Option	Description
<i>offline</i>	Offline.
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.

port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15

port2-mode	LAN port 2 mode.	option	-

Option	Description
<i>offline</i>	Offline.
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.

port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15

port3-mode	LAN port 3 mode.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
	Option	Description											
	<i>offline</i>	Offline.											
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.											
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.											
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15										
port4-mode	LAN port 4 mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
	Option	Description											
	<i>offline</i>	Offline.											
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.											
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.											
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15										
port5-mode	LAN port 5 mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
	Option	Description											
	<i>offline</i>	Offline.											
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.											
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.											
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15										
port6-mode	LAN port 6 mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
	Option	Description											
	<i>offline</i>	Offline.											
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.											
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.											
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												

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	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15
port8-mode	LAN port 8 mode.	option	-
	Option	Description	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15

config radio-1

Parameter	Description	Type	Size
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable automatic transmit power adjustment.	
	<i>disable</i>	Disable automatic transmit power adjustment.	

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
band	WiFi band that Radio 1 operates on.	option	-

Option	Description
<i>802.11a</i>	802.11a.
<i>802.11b</i>	802.11b.
<i>802.11g</i>	802.11g/b.
<i>802.11n</i>	802.11n/g/b radio at 2.4GHz band.
<i>802.11n-5G</i>	802.11n/a at 5GHz.
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.
<i>802.11g-only</i>	802.11g.
<i>802.11n-only</i>	802.11n at 2.4GHz.
<i>802.11n-5G-only</i>	802.11n at 5GHz.
<i>802.11ac</i>	802.11ac/n/a radio.
<i>802.11ac,n-only</i>	802.11ac/n.
<i>802.11ac-only</i>	802.11ac.
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.
<i>802.11ax-only</i>	802.11ax at 2.4GHz.

channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3
override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Override the WTP profile spectrum analysis configuration.	
	<i>disable</i>	Use the WTP profile spectrum analysis configuration.	
override-band	Enable to override the WTP profile band setting.	option	-
	Option	Description	
	<i>enable</i>	Override the WTP profile band setting.	
	<i>disable</i>	Use the WTP profile band setting.	
override-channel	Enable to override WTP profile channel settings.	option	-
	Option	Description	
	<i>enable</i>	Override WTP profile channel settings.	
	<i>disable</i>	Use WTP profile channel settings.	
override-tpower	Enable to override the WTP profile power level configuration.	option	-
	Option	Description	
	<i>enable</i>	Override the WTP profile power level configuration.	
	<i>disable</i>	Use the WTP profile power level configuration.	
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-
	Option	Description	
	<i>enable</i>	Override WTP profile VAP settings.	
	<i>disable</i>	Use WTP profile VAP settings.	
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable spectrum analysis.	
	<i>disable</i>	Disable spectrum analysis.	
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Automatically select tunnel VAPs.	
	<i>disable</i>	Manually select VAPs.	
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35

config radio-2

Parameter	Description	Type	Size
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable automatic transmit power adjustment.	
	<i>disable</i>	Disable automatic transmit power adjustment.	
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295
band	WiFi band that Radio 2 operates on.	option	-
	Option	Description	
	<i>802.11a</i>	802.11a.	

Parameter	Description	Type	Size

Option	Description
<i>802.11b</i>	802.11b.
<i>802.11g</i>	802.11g/b.
<i>802.11n</i>	802.11n/g/b radio at 2.4GHz band.
<i>802.11n-5G</i>	802.11n/a at 5GHz.
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.
<i>802.11g-only</i>	802.11g.
<i>802.11n-only</i>	802.11n at 2.4GHz.
<i>802.11n-5G-only</i>	802.11n at 5GHz.
<i>802.11ac</i>	802.11ac/n/a radio.
<i>802.11ac,n-only</i>	802.11ac/n.
<i>802.11ac-only</i>	802.11ac.
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.
<i>802.11ax-only</i>	802.11ax at 2.4GHz.

channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3
override- analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-

Option	Description
<i>enable</i>	Override the WTP profile spectrum analysis configuration.
<i>disable</i>	Use the WTP profile spectrum analysis configuration.

override-band	Enable to override the WTP profile band setting.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Override the WTP profile band setting.	
	<i>disable</i>	Use the WTP profile band setting.	
override-channel	Enable to override WTP profile channel settings.	option	-
	Option	Description	
	<i>enable</i>	Override WTP profile channel settings.	
	<i>disable</i>	Use WTP profile channel settings.	
override-tpower	Enable to override the WTP profile power level configuration.	option	-
	Option	Description	
	<i>enable</i>	Override the WTP profile power level configuration.	
	<i>disable</i>	Use the WTP profile power level configuration.	
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-
	Option	Description	
	<i>enable</i>	Override WTP profile VAP settings.	
	<i>disable</i>	Use WTP profile VAP settings.	
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-
	Option	Description	
	<i>enable</i>	Enable spectrum analysis.	
	<i>disable</i>	Disable spectrum analysis.	
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Automatically select tunnel VAPs.	
	<i>disable</i>	Manually select VAPs.	
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35

config radio-3

Parameter	Description	Type	Size
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable automatic transmit power adjustment.	
	<i>disable</i>	Disable automatic transmit power adjustment.	
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295
band	WiFi band that Radio 3 operates on.	option	-
	Option	Description	
	<i>802.11a</i>	802.11a.	
	<i>802.11b</i>	802.11b.	
	<i>802.11g</i>	802.11g/b.	
	<i>802.11n</i>	802.11n/g/b radio at 2.4GHz band.	
	<i>802.11n-5G</i>	802.11n/a at 5GHz.	
	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	

Parameter	Description	Type	Size																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11g-only</td><td>802.11g.</td></tr><tr><td>802.11n-only</td><td>802.11n at 2.4GHz.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n at 5GHz.</td></tr><tr><td>802.11ac</td><td>802.11ac/n/a radio.</td></tr><tr><td>802.11ac,n-only</td><td>802.11ac/n.</td></tr><tr><td>802.11ac-only</td><td>802.11ac.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	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.		
	Option	Description																															
	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.																																
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3																														
override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile spectrum analysis configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile spectrum analysis configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile spectrum analysis configuration.	disable	Use the WTP profile spectrum analysis configuration.																										
	Option	Description																															
	enable	Override the WTP profile spectrum analysis configuration.																															
disable	Use the WTP profile spectrum analysis configuration.																																
override-band	Enable to override the WTP profile band setting.	option	-																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile band setting.</td></tr><tr><td>disable</td><td>Use the WTP profile band setting.</td></tr></table>	Option	Description	enable	Override the WTP profile band setting.	disable	Use the WTP profile band setting.																										
	Option	Description																															
	enable	Override the WTP profile band setting.																															
disable	Use the WTP profile band setting.																																
override-channel	Enable to override WTP profile channel settings.	option	-																														

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Override WTP profile channel settings.	
	<i>disable</i>	Use WTP profile channel settings.	
override-tpower	Enable to override the WTP profile power level configuration.	option	-
	Option	Description	
	<i>enable</i>	Override the WTP profile power level configuration.	
	<i>disable</i>	Use the WTP profile power level configuration.	
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-
	Option	Description	
	<i>enable</i>	Override WTP profile VAP settings.	
	<i>disable</i>	Use WTP profile VAP settings.	
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-
	Option	Description	
	<i>enable</i>	Enable spectrum analysis.	
	<i>disable</i>	Disable spectrum analysis.	
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Automatically select tunnel VAPs.	
	<i>disable</i>	Manually select VAPs.	
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35

config radio-4

Parameter	Description	Type	Size
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable automatic transmit power adjustment.	
	<i>disable</i>	Disable automatic transmit power adjustment.	
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295
band	WiFi band that Radio 4 operates on.	option	-

Option	Description
<i>802.11a</i>	802.11a.
<i>802.11b</i>	802.11b.
<i>802.11g</i>	802.11g/b.
<i>802.11n</i>	802.11n/g/b radio at 2.4GHz band.
<i>802.11n-5G</i>	802.11n/a at 5GHz.
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.
<i>802.11g-only</i>	802.11g.
<i>802.11n-only</i>	802.11n at 2.4GHz.
<i>802.11n-5G-only</i>	802.11n at 5GHz.
<i>802.11ac</i>	802.11ac/n/a radio.
<i>802.11ac,n-only</i>	802.11ac/n.
<i>802.11ac-only</i>	802.11ac.
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.

Parameter	Description	Type	Size														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	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.		
	Option	Description															
	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.																
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3														
override-analysis	Enable to override the WTP profile spectrum analysis configuration.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile spectrum analysis configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile spectrum analysis configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile spectrum analysis configuration.	disable	Use the WTP profile spectrum analysis configuration.										
	Option	Description															
	enable	Override the WTP profile spectrum analysis configuration.															
disable	Use the WTP profile spectrum analysis configuration.																
override-band	Enable to override the WTP profile band setting.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile band setting.</td></tr><tr><td>disable</td><td>Use the WTP profile band setting.</td></tr></table>	Option	Description	enable	Override the WTP profile band setting.	disable	Use the WTP profile band setting.										
	Option	Description															
	enable	Override the WTP profile band setting.															
disable	Use the WTP profile band setting.																
override-channel	Enable to override WTP profile channel settings.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override WTP profile channel settings.</td></tr><tr><td>disable</td><td>Use WTP profile channel settings.</td></tr></table>	Option	Description	enable	Override WTP profile channel settings.	disable	Use WTP profile channel settings.										
	Option	Description															
	enable	Override WTP profile channel settings.															
disable	Use WTP profile channel settings.																
override-tpower	Enable to override the WTP profile power level configuration.	option	-														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile power level configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile power level configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile power level configuration.	disable	Use the WTP profile power level configuration.										
	Option	Description															
	enable	Override the WTP profile power level configuration.															
disable	Use the WTP profile power level configuration.																
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-														

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override WTP profile VAP settings.</td></tr><tr><td><i>disable</i></td><td>Use WTP profile VAP settings.</td></tr></table>	Option	Description	<i>enable</i>	Override WTP profile VAP settings.	<i>disable</i>	Use WTP profile VAP settings.		
Option	Description								
<i>enable</i>	Override WTP profile VAP settings.								
<i>disable</i>	Use WTP profile VAP settings.								
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100						
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable spectrum analysis.</td></tr><tr><td><i>disable</i></td><td>Disable spectrum analysis.</td></tr></table>	Option	Description	<i>enable</i>	Enable spectrum analysis.	<i>disable</i>	Disable spectrum analysis.		
Option	Description								
<i>enable</i>	Enable spectrum analysis.								
<i>disable</i>	Disable spectrum analysis.								
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Automatically select tunnel VAPs.</td></tr><tr><td><i>disable</i></td><td>Manually select VAPs.</td></tr></table>	Option	Description	<i>enable</i>	Automatically select tunnel VAPs.	<i>disable</i>	Manually select VAPs.		
Option	Description								
<i>enable</i>	Automatically select tunnel VAPs.								
<i>disable</i>	Manually select VAPs.								
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35						

config split-tunneling-acl

Parameter	Description	Type	Size
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295

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
name	WTP group name.	string	Maximum length: 35
platform-type	FortiAP models to define the WTP group platform type.	option	-

Option	Description
<i>AP-11N</i>	Default 11n AP.
<i>220B</i>	FAP220B/221B.
<i>210B</i>	FAP210B.
<i>222B</i>	FAP222B.
<i>112B</i>	FAP112B.
<i>320B</i>	FAP320B.
<i>11C</i>	FAP11C.
<i>14C</i>	FAP14C.
<i>223B</i>	FAP223B.
<i>28C</i>	FAP28C.
<i>320C</i>	FAP320C.
<i>221C</i>	FAP221C.
<i>25D</i>	FAP25D.
<i>222C</i>	FAP222C.
<i>224D</i>	FAP224D.
<i>214B</i>	FK214B.
<i>21D</i>	FAP21D.
<i>24D</i>	FAP24D.
<i>112D</i>	FAP112D.
<i>223C</i>	FAP223C.

Parameter	Description	Type	Size

Option	Description
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.
231E	FAP231E.
S221E	FAPS221E.
S223E	FAPS223E.
321E	FAP321E.
431F	FAP431F.
432F	FAP432F.
433F	FAP433F.

Parameter	Description	Type	Size

Option	Description
<i>231F</i>	FAP231F.
<i>234F</i>	FAP234F.
<i>23JF</i>	FAP23JF.
<i>U421E</i>	FAPU421EV.
<i>U422EV</i>	FAPU422EV.
<i>U423E</i>	FAPU423EV.
<i>U221EV</i>	FAPU221EV.
<i>U223EV</i>	FAPU223EV.
<i>U24JEV</i>	FAPU24JEV.
<i>U321EV</i>	FAPU321EV.
<i>U323EV</i>	FAPU323EV.
<i>U431F</i>	FAPU431F.
<i>U433F</i>	FAPU433F.

wtps <wtp-id>	WTP list. WTP ID.	string	Maximum length: 35

config wireless-controller wtp-profile

Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```
config wireless-controller wtp-profile
```

Description: Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```
edit <name>
```

```
set allowaccess {option1}, {option2}, ...
```

```
set ap-country [NA|AL|...]
```

```
set ble-profile {string}
```

```
set comment {var-string}
```

```
set control-message-offload {option1}, {option2}, ...
```

```
config deny-mac-list
```

Description: List of MAC addresses that are denied access to this WTP, FortiAP, or AP.

```
edit <id>
```

```
set mac {mac-address}
```

```
next
```

```
end
```

```
set dtls-in-kernel [enable|disable]
```

```
set dtls-policy {option1}, {option2}, ...
```

```
set energy-efficient-ethernet [enable|disable]
```



```

set ext-info-enable [enable|disable]
set handoff-roaming [enable|disable]
set handoff-rssi {integer}
set handoff-sta-thresh {integer}
set ip-fragment-preventing {option1}, {option2}, ...
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
config lbs
    Description: Set various location based service (LBS) options.
    set aeroscout [enable|disable]
    set aeroscout-ap-mac [bssid|board-mac]
    set aeroscout-mmu-report [enable|disable]
    set aeroscout-mu [enable|disable]
    set aeroscout-mu-factor {integer}
    set aeroscout-mu-timeout {integer}
    set aeroscout-server-ip {ipv4-address-any}
    set aeroscout-server-port {integer}
    set ekahau-blink-mode [enable|disable]
    set ekahau-tag {mac-address}
    set erc-server-ip {ipv4-address-any}
    set erc-server-port {integer}
    set fortipresence [foreign|both|...]
    set fortipresence-ble [enable|disable]
    set fortipresence-frequency {integer}
    set fortipresence-port {integer}
    set fortipresence-project {string}
    set fortipresence-rogue [enable|disable]
    set fortipresence-secret {password}
    set fortipresence-server {ipv4-address-any}
    set fortipresence-unassoc [enable|disable]
    set station-locate [enable|disable]
end
set led-schedules <name1>, <name2>, ...
set led-state [enable|disable]
set lldp [enable|disable]
set login-passwd {password}
set login-passwd-change [yes|default|...]

```

```

set max-clients {integer}
config platform
    Description: WTP, FortiAP, or AP platform.
    set ddscan [enable|disable]
    set mode [single-5G|dual-5G]
    set type [AP-11N|220B|...]
end
set poe-mode [auto|8023af|...]
config radio-1
    Description: Configuration options for radio 1.
    set airtime-fairness [enable|disable]
    set amsdu [enable|disable]
    set ap-handoff [enable|disable]
    set ap-sniffer-addr {mac-address}
    set ap-sniffer-bufsize {integer}
    set ap-sniffer-chan {integer}
    set ap-sniffer-ctl [enable|disable]
    set ap-sniffer-data [enable|disable]
    set ap-sniffer-mgmt-beacon [enable|disable]
    set ap-sniffer-mgmt-other [enable|disable]
    set ap-sniffer-mgmt-probe [enable|disable]
    set auto-power-high {integer}
    set auto-power-level [enable|disable]
    set auto-power-low {integer}
    set band [802.11a|802.11b|...]
    set band-5g-type [5g-full|5g-high|...]
    set bandwidth-admission-control [enable|disable]
    set bandwidth-capacity {integer}
    set beacon-interval {integer}
    set call-admission-control [enable|disable]
    set call-capacity {integer}
    set channel <chan1>, <chan2>, ...
    set channel-bonding [160MHz|80MHz|...]
    set channel-utilization [enable|disable]
    set coexistence [enable|disable]
    set darrp [enable|disable]
    set dtim {integer}
    set frag-threshold {integer}
    set frequency-handoff [enable|disable]
    set max-clients {integer}
    set max-distance {integer}
    set mode [disabled|ap|...]
    set power-level {integer}
    set powersave-optimize {option1}, {option2}, ...
    set protection-mode [rtscts|ctsonly|...]
    set rts-threshold {integer}
    set short-guard-interval [enable|disable]
    set spectrum-analysis [enable|disable]
    set transmit-optimize {option1}, {option2}, ...
    set vap-all [enable|disable]
    set vaps <name1>, <name2>, ...
    set wids-profile {string}
    set zero-wait-dfs [enable|disable]
end
config radio-2
    Description: Configuration options for radio 2.

```

```

set airtime-fairness [enable|disable]
set amsdu [enable|disable]
set ap-handoff [enable|disable]
set ap-sniffer-addr {mac-address}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set auto-power-high {integer}
set auto-power-level [enable|disable]
set auto-power-low {integer}
set band [802.11a|802.11b|...]
set band-5g-type [5g-full|5g-high|...]
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
set beacon-interval {integer}
set call-admission-control [enable|disable]
set call-capacity {integer}
set channel <chan1>, <chan2>, ...
set channel-bonding [160MHz|80MHz|...]
set channel-utilization [enable|disable]
set coexistence [enable|disable]
set darrp [enable|disable]
set dtim {integer}
set frag-threshold {integer}
set frequency-handoff [enable|disable]
set max-clients {integer}
set max-distance {integer}
set mode [disabled|ap|...]
set power-level {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set short-guard-interval [enable|disable]
set spectrum-analysis [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [enable|disable]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config radio-3
  Description: Configuration options for radio 3.
  set airtime-fairness [enable|disable]
  set amsdu [enable|disable]
  set ap-handoff [enable|disable]
  set ap-sniffer-addr {mac-address}
  set ap-sniffer-bufsize {integer}
  set ap-sniffer-chan {integer}
  set ap-sniffer-ctl [enable|disable]
  set ap-sniffer-data [enable|disable]
  set ap-sniffer-mgmt-beacon [enable|disable]
  set ap-sniffer-mgmt-other [enable|disable]

```

```

set ap-sniffer-mgmt-probe [enable|disable]
set auto-power-high {integer}
set auto-power-level [enable|disable]
set auto-power-low {integer}
set band [802.11a|802.11b|...]
set band-5g-type [5g-full|5g-high|...]
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
set beacon-interval {integer}
set call-admission-control [enable|disable]
set call-capacity {integer}
set channel <chan1>, <chan2>, ...
set channel-bonding [160MHz|80MHz|...]
set channel-utilization [enable|disable]
set coexistence [enable|disable]
set darrp [enable|disable]
set dtim {integer}
set frag-threshold {integer}
set frequency-handoff [enable|disable]
set max-clients {integer}
set max-distance {integer}
set mode [disabled|ap|...]
set power-level {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set short-guard-interval [enable|disable]
set spectrum-analysis [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [enable|disable]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config radio-4
Description: Configuration options for radio 4.
set airtime-fairness [enable|disable]
set amsdu [enable|disable]
set ap-handoff [enable|disable]
set ap-sniffer-addr {mac-address}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set auto-power-high {integer}
set auto-power-level [enable|disable]
set auto-power-low {integer}
set band [802.11a|802.11b|...]
set band-5g-type [5g-full|5g-high|...]
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
set beacon-interval {integer}
set call-admission-control [enable|disable]

```

```

set call-capacity {integer}
set channel <chan1>, <chan2>, ...
set channel-bonding [160MHz|80MHz|...]
set channel-utilization [enable|disable]
set coexistence [enable|disable]
set darrp [enable|disable]
set dtim {integer}
set frag-threshold {integer}
set frequency-handoff [enable|disable]
set max-clients {integer}
set max-distance {integer}
set mode [disabled|ap|...]
set power-level {integer}
set powersave-optimize {option1}, {option2}, ...
set protection-mode [rtscts|ctsonly|...]
set rts-threshold {integer}
set short-guard-interval [enable|disable]
set spectrum-analysis [enable|disable]
set transmit-optimize {option1}, {option2}, ...
set vap-all [enable|disable]
set vaps <name1>, <name2>, ...
set wids-profile {string}
set zero-wait-dfs [enable|disable]
end
config split-tunneling-acl
  Description: Split tunneling ACL filter list.
  edit <id>
    set dest-ip {ipv4-classnet}
  next
end
set split-tunneling-acl-local-ap-subnet [enable|disable]
set split-tunneling-acl-path [tunnel|local]
set tun-mtu-downlink {integer}
set tun-mtu-uplink {integer}
set wan-port-mode [wan-lan|wan-only]
next
end

```

config wireless-controller wtp-profile

Parameter	Description	Type	Size
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.	

Parameter	Description	Type	Size
ap-country	Country in which this WTP, FortiAP or AP will operate (default = NA, automatically use the country configured for the current VDOM).	option	-

Option	Description
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
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

Parameter	Description	Type	Size

Option	Description
<i>CR</i>	COSTA RICA
<i>HR</i>	CROATIA
<i>CY</i>	CYPRUS
<i>CZ</i>	CZECH REPUBLIC
<i>DK</i>	DENMARK
<i>DO</i>	DOMINICAN REPUBLIC
<i>EC</i>	ECUADOR
<i>EG</i>	EGYPT
<i>SV</i>	EL SALVADOR
<i>EE</i>	ESTONIA
<i>FI</i>	FINLAND
<i>FR</i>	FRANCE
<i>GE</i>	GEORGIA
<i>DE</i>	GERMANY
<i>GR</i>	GREECE
<i>GL</i>	GREENLAND
<i>GD</i>	GRENADA
<i>GU</i>	GUAM
<i>GT</i>	GUATEMALA
<i>HT</i>	HAITI
<i>HN</i>	HONDURAS
<i>HK</i>	HONG KONG
<i>HU</i>	HUNGARY
<i>IS</i>	ICELAND
<i>IN</i>	INDIA
<i>ID</i>	INDONESIA
<i>IR</i>	IRAN
<i>IE</i>	IRELAND
<i>IL</i>	ISRAEL

Parameter	Description	Type	Size

Option	Description
<i>IT</i>	ITALY
<i>JM</i>	JAMAICA
<i>JO</i>	JORDAN
<i>KZ</i>	KAZAKHSTAN
<i>KE</i>	KENYA
<i>KP</i>	NORTH KOREA
<i>KR</i>	KOREA REPUBLIC
<i>KW</i>	KUWAIT
<i>LV</i>	LATVIA
<i>LB</i>	LEBANON
<i>LI</i>	LIECHTENSTEIN
<i>LT</i>	LITHUANIA
<i>LU</i>	LUXEMBOURG
<i>MO</i>	MACAU SAR
<i>MK</i>	MACEDONIA, FYRO
<i>MY</i>	MALAYSIA
<i>MT</i>	MALTA
<i>MX</i>	MEXICO
<i>MC</i>	MONACO
<i>MA</i>	MOROCCO
<i>MZ</i>	MOZAMBIQUE
<i>MM</i>	MYANMAR
<i>NP</i>	NEPAL
<i>NL</i>	NETHERLANDS
<i>AN</i>	NETHERLANDS ANTILLES
<i>AW</i>	ARUBA
<i>NZ</i>	NEW ZEALAND
<i>NO</i>	NORWAY
<i>OM</i>	OMAN

Parameter	Description	Type	Size

Option	Description
<i>PK</i>	PAKISTAN
<i>PA</i>	PANAMA
<i>PG</i>	PAPUA NEW GUINEA
<i>PY</i>	PARAGUAY
<i>PE</i>	PERU
<i>PH</i>	PHILIPPINES
<i>PL</i>	POLAND
<i>PT</i>	PORTUGAL
<i>PR</i>	PUERTO RICO
<i>QA</i>	QATAR
<i>RO</i>	ROMANIA
<i>RU</i>	RUSSIA
<i>RW</i>	RWANDA
<i>SA</i>	SAUDI ARABIA
<i>RS</i>	REPUBLIC OF SERBIA
<i>ME</i>	MONTENEGRO
<i>SG</i>	SINGAPORE
<i>SK</i>	SLOVAKIA
<i>SI</i>	SLOVENIA
<i>ZA</i>	SOUTH AFRICA
<i>ES</i>	SPAIN
<i>LK</i>	SRI LANKA
<i>SE</i>	SWEDEN
<i>SD</i>	SUDAN
<i>CH</i>	SWITZERLAND
<i>SY</i>	SYRIAN ARAB REPUBLIC
<i>TW</i>	TAIWAN
<i>TZ</i>	TANZANIA
<i>TH</i>	THAILAND

Parameter	Description	Type	Size

Option	Description
<i>TT</i>	TRINIDAD AND TOBAGO
<i>TN</i>	TUNISIA
<i>TR</i>	TURKEY
<i>AE</i>	UNITED ARAB EMIRATES
<i>UA</i>	UKRAINE
<i>GB</i>	UNITED KINGDOM
<i>US</i>	UNITED STATES2
<i>PS</i>	UNITED STATES (PUBLIC SAFETY)
<i>UY</i>	URUGUAY
<i>UZ</i>	UZBEKISTAN
<i>VE</i>	VENEZUELA
<i>VN</i>	VIET NAM
<i>YE</i>	YEMEN
<i>ZB</i>	ZAMBIA
<i>ZW</i>	ZIMBABWE
<i>JP</i>	JAPAN14
<i>CA</i>	CANADA2

ble-profile	Bluetooth Low Energy profile name.	string	Maximum length: 35
comment	Comment.	var-string	Maximum length: 255
control-message-offload	Enable/disable CAPWAP control message data channel offload.	option	-

Option	Description
<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.
<i>aeroscout-tag</i>	AeroScout tag.
<i>ap-list</i>	Rogue AP list.
<i>sta-list</i>	Rogue STA list.

Parameter	Description	Type	Size
	Option	Description	
	<i>sta-cap-list</i>	STA capability list.	
	<i>stats</i>	WTP, radio, VAP, and STA statistics.	
	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	
	<i>sta-health</i>	STA health log.	
dtls-in-kernel	Enable/disable data channel DTLS in kernel.	option	-
	Option	Description	
	<i>enable</i>	Enable data channel DTLS in kernel.	
	<i>disable</i>	Disable data channel DTLS in kernel.	
dtls-policy	WTP data channel DTLS policy (default = clear-text).	option	-
	Option	Description	
	<i>clear-text</i>	Clear Text Data Channel.	
	<i>dtls-enabled</i>	DTLS Enabled Data Channel.	
	<i>ipsec-vpn</i>	IPsec VPN Data Channel.	
energy-efficient-ethernet	Enable/disable use of energy efficient Ethernet on WTP.	option	-
	Option	Description	
	<i>enable</i>	Enable use of energy efficient Ethernet on WTP.	
	<i>disable</i>	Disable use of energy efficient Ethernet on WTP.	
ext-info-enable	Enable/disable station/VAP/radio extension information.	option	-
	Option	Description	
	<i>enable</i>	Enable station/VAP/radio extension information.	
	<i>disable</i>	Disable station/VAP/radio extension information.	
handoff-roaming	Enable/disable client load balancing during roaming to avoid roaming delay (default = disable).	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable handoff roaming.</td></tr><tr><td><i>disable</i></td><td>Disable handoff roaming.</td></tr></table>	Option	Description	<i>enable</i>	Enable handoff roaming.	<i>disable</i>	Disable handoff roaming.		
Option	Description								
<i>enable</i>	Enable handoff roaming.								
<i>disable</i>	Disable handoff roaming.								
handoff-rssi	Minimum received signal strength indicator (RSSI) value for handoff (20 - 30, default = 25).	integer	Minimum value: 20 Maximum value: 30						
handoff-sta-thresh	Threshold value for AP handoff.	integer	Minimum value: 0 Maximum value: 4294967295						
ip-fragment-preventing	Method(s) by which IP fragmentation is prevented for control and data packets through CAPWAP tunnel (default = tcp-mss-adjust).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-mss-adjust</i></td><td>TCP maximum segment size adjustment.</td></tr><tr><td><i>icmp-unreachable</i></td><td>Drop packet and send ICMP Destination Unreachable</td></tr></table>	Option	Description	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable		
Option	Description								
<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.								
<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable								
led-schedules <name>	Recurring firewall schedules for illuminating LEDs on the FortiAP. If led-state is enabled, LEDs will be visible when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35						
led-state	Enable/disable use of LEDs on WTP (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of LEDs on WTP.</td></tr><tr><td><i>disable</i></td><td>Disable use of LEDs on WTP.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of LEDs on WTP.	<i>disable</i>	Disable use of LEDs on WTP.		
Option	Description								
<i>enable</i>	Enable use of LEDs on WTP.								
<i>disable</i>	Disable use of LEDs on WTP.								
lldp	Enable/disable Link Layer Discovery Protocol (LLDP) for the WTP, FortiAP, or AP (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable LLDP.</td></tr><tr><td><i>disable</i></td><td>Disable LLDP.</td></tr></table>	Option	Description	<i>enable</i>	Enable LLDP.	<i>disable</i>	Disable LLDP.		
Option	Description								
<i>enable</i>	Enable LLDP.								
<i>disable</i>	Disable LLDP.								

Parameter	Description	Type	Size
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP (yes, default, or no, default = no).	option	-
	Option	Description	
	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.	
	<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	
	<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.	
max-clients	Maximum number of stations (STAs) supported by the WTP (default = 0, meaning no client limitation).	integer	Minimum value: 0 Maximum value: 4294967295
name	WTP (or FortiAP or AP) profile name.	string	Maximum length: 35
poe-mode	Set the WTP, FortiAP, or AP's PoE mode.	option	-
	Option	Description	
	<i>auto</i>	Automatically detect the PoE mode.	
	<i>8023af</i>	Use 802.3af PoE mode.	
	<i>8023at</i>	Use 802.3at PoE mode.	
	<i>power-adapter</i>	Use the power adapter to control the PoE mode.	
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	
	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.	
	<i>local</i>	Split tunneling ACL list traffic will be local NATed.	
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 576 Maximum value: 1500
tun-mtu-uplink	The maximum transmission unit (MTU) of uplink CAPWAP tunnel (576 - 1500 bytes or 0; 0 means the local MTU of FortiAP; default = 0).	integer	Minimum value: 576 Maximum value: 1500
wan-port-mode	Enable/disable using a WAN port as a LAN port.	option	-
	Option	Description	
	<i>wan-lan</i>	Enable using a WAN port as a LAN port.	
	<i>wan-only</i>	Disable using a WAN port as a LAN port.	

config deny-mac-list

Parameter	Description	Type	Size
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295
mac	A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.	mac-address	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.	

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.								
Option	Description												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15										
port1-mode	LAN port 1 mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
Option	Description												
<i>offline</i>	Offline.												
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15										
port2-mode	LAN port 2 mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
Option	Description												
<i>offline</i>	Offline.												
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15										
port3-mode	LAN port 3 mode.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
Option	Description												
<i>offline</i>	Offline.												
<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.												
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15										
port4-mode	LAN port 4 mode.	option	-										

Parameter	Description	Type	Size
	Option	Description	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15
port5-mode	LAN port 5 mode.	option	-
	Option	Description	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15
port6-mode	LAN port 6 mode.	option	-
	Option	Description	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15
port7-mode	LAN port 7 mode.	option	-
	Option	Description	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	

Parameter	Description	Type	Size
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15
port8-mode	LAN port 8 mode.	option	-
	Option	Description	
	<i>offline</i>	Offline.	
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.	
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15

config lbs

Parameter	Description	Type	Size						
aeroscout	Enable/disable AeroScout Real Time Location Service (RTLS) support (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AeroScout support.</td></tr><tr><td><i>disable</i></td><td>Disable AeroScout support.</td></tr></table>	Option	Description	<i>enable</i>	Enable AeroScout support.	<i>disable</i>	Disable AeroScout support.		
Option	Description								
<i>enable</i>	Enable AeroScout support.								
<i>disable</i>	Disable AeroScout support.								
aeroscout-ap-mac	Use BSSID or board MAC address as AP MAC address in AeroScout AP messages (default = bssid).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bssid</i></td><td>Use BSSID as AP MAC address in AeroScout AP messages.</td></tr><tr><td><i>board-mac</i></td><td>Use board MAC address as AP MAC address in AeroScout AP messages.</td></tr></table>	Option	Description	<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.	<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.		
Option	Description								
<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.								
<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.								
aeroscout-mmu-report	Enable/disable compounded AeroScout tag and MU report (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable compounded AeroScout tag and MU report.</td></tr><tr><td><i>disable</i></td><td>Disable compounded AeroScout tag and MU report.</td></tr></table>	Option	Description	<i>enable</i>	Enable compounded AeroScout tag and MU report.	<i>disable</i>	Disable compounded AeroScout tag and MU report.		
Option	Description								
<i>enable</i>	Enable compounded AeroScout tag and MU report.								
<i>disable</i>	Disable compounded AeroScout tag and MU report.								
aeroscout-mu	Enable/disable AeroScout Mobile Unit (MU) support (default = disable).	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AeroScout MU mode support.</td></tr><tr><td><i>disable</i></td><td>Disable AeroScout MU mode support.</td></tr></table>	Option	Description	<i>enable</i>	Enable AeroScout MU mode support.	<i>disable</i>	Disable AeroScout MU mode support.		
	Option	Description							
	<i>enable</i>	Enable AeroScout MU mode support.							
<i>disable</i>	Disable AeroScout MU mode support.								
aeroscout-mu-factor	AeroScout MU mode dilution factor (default = 20).	integer	Minimum value: 0 Maximum value: 4294967295						
aeroscout-mu-timeout	AeroScout MU mode timeout (0 - 65535 sec, default = 5).	integer	Minimum value: 0 Maximum value: 65535						
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						
ekahau-blink-mode	Enable/disable Ekahau blink mode (now known as AiRISTA Flow) to track and locate WiFi tags (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Ekahau blink mode.</td></tr><tr><td><i>disable</i></td><td>Disable Ekahau blink mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable Ekahau blink mode.	<i>disable</i>	Disable Ekahau blink mode.		
	Option	Description							
	<i>enable</i>	Enable Ekahau blink mode.							
<i>disable</i>	Disable Ekahau blink mode.								
ekahau-tag	WiFi frame MAC address or WiFi Tag.	mac-address	Not Specified						
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						
fortipresence	Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network (default = disable).	option	-						

Parameter	Description	Type	Size

	Option	Description	
	<i>foreign</i>	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.	
	<i>both</i>	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.	
	<i>disable</i>	Disable FortiPresence.	

fortipresence-ble	Enable/disable FortiPresence finding and reporting BLE devices.	option	-

	Option	Description	
	<i>enable</i>	Enable FortiPresence finding and reporting BLE devices.	
	<i>disable</i>	Disable FortiPresence finding and reporting BLE devices.	

fortipresence-frequency	FortiPresence report transmit frequency (5 - 65535 sec, default = 30).	integer	Minimum value: 5 Maximum value: 65535

fortipresence-port	FortiPresence server UDP listening port (default = 3000).	integer	Minimum value: 300 Maximum value: 65535

fortipresence-project	FortiPresence project name (max. 16 characters, default = fortipresence).	string	Maximum length: 16

fortipresence-rogue	Enable/disable FortiPresence finding and reporting rogue APs.	option	-

	Option	Description	
	<i>enable</i>	Enable FortiPresence finding and reporting rogue APs.	
	<i>disable</i>	Disable FortiPresence finding and reporting rogue APs.	

fortipresence-secret	FortiPresence secret password (max. 16 characters).	password	Not Specified

fortipresence-server	FortiPresence server IP address.	ipv4-address-any	Not Specified

fortipresence-unassoc	Enable/disable FortiPresence finding and reporting unassociated stations.	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable FortiPresence finding and reporting unassociated stations.	
	<i>disable</i>	Disable FortiPresence finding and reporting unassociated stations.	
station-locate	Enable/disable client station locating services for all clients, whether associated or not (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable station locating service.	
	<i>disable</i>	Disable station locating service.	

config platform

Parameter	Description	Type	Size						
ddscan	Enable/disable use of one radio for dedicated dual-band scanning to detect RF characterization and wireless threat management.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dedicated dual-band scan mode.</td></tr><tr><td><i>disable</i></td><td>Disable dedicated dual-band scan mode.</td></tr></table>			Option	Description	<i>enable</i>	Enable dedicated dual-band scan mode.	<i>disable</i>	Disable dedicated dual-band scan mode.
Option	Description								
<i>enable</i>	Enable dedicated dual-band scan mode.								
<i>disable</i>	Disable dedicated dual-band scan mode.								
mode	Configure operation mode of 5G radios (default = single-5G).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single-5G</i></td><td>Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.</td></tr><tr><td><i>dual-5G</i></td><td>Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.</td></tr></table>			Option	Description	<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.	<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.
Option	Description								
<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.								
<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.								
type	WTP, FortiAP or AP platform type. There are built-in WTP profiles for all supported FortiAP models. You can select a built-in profile and customize it or create a new profile.	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>AP-11N</i></td><td>Default 11n AP.</td></tr></table>			Option	Description	<i>AP-11N</i>	Default 11n AP.		
Option	Description								
<i>AP-11N</i>	Default 11n AP.								

Parameter	Description	Type	Size

Option	Description
220B	FAP220B/221B.
210B	FAP210B.
222B	FAP222B.
112B	FAP112B.
320B	FAP320B.
11C	FAP11C.
14C	FAP14C.
223B	FAP223B.
28C	FAP28C.
320C	FAP320C.
221C	FAP221C.
25D	FAP25D.
222C	FAP222C.
224D	FAP224D.
214B	FK214B.
21D	FAP21D.
24D	FAP24D.
112D	FAP112D.
223C	FAP223C.
321C	FAP321C.
C220C	FAPC220C.
C225C	FAPC225C.
C23JD	FAPC23JD.
C24JE	FAPC24JE.
S321C	FAPS321C.
S322C	FAPS322C.
S323C	FAPS323C.
S311C	FAPS311C.
S313C	FAPS313C.

Parameter	Description	Type	Size

Option	Description
<i>S321CR</i>	FAPS321CR.
<i>S322CR</i>	FAPS322CR.
<i>S323CR</i>	FAPS323CR.
<i>S421E</i>	FAPS421E.
<i>S422E</i>	FAPS422E.
<i>S423E</i>	FAPS423E.
<i>421E</i>	FAP421E.
<i>423E</i>	FAP423E.
<i>221E</i>	FAP221E.
<i>222E</i>	FAP222E.
<i>223E</i>	FAP223E.
<i>224E</i>	FAP224E.
<i>231E</i>	FAP231E.
<i>S221E</i>	FAPS221E.
<i>S223E</i>	FAPS223E.
<i>321E</i>	FAP321E.
<i>431F</i>	FAP431F.
<i>432F</i>	FAP432F.
<i>433F</i>	FAP433F.
<i>231F</i>	FAP231F.
<i>234F</i>	FAP234F.
<i>23JF</i>	FAP23JF.
<i>U421E</i>	FAPU421EV.
<i>U422EV</i>	FAPU422EV.
<i>U423E</i>	FAPU423EV.
<i>U221EV</i>	FAPU221EV.
<i>U223EV</i>	FAPU223EV.
<i>U24JEV</i>	FAPU24JEV.
<i>U321EV</i>	FAPU321EV.

Parameter	Description	Type	Size
	Option	Description	
	<i>U323EV</i>	FAPU323EV.	
	<i>U431F</i>	FAPU431F.	
	<i>U433F</i>	FAPU433F.	

config radio-1

Parameter	Description	Type	Size
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable airtime fairness (ATF) support.	
	<i>disable</i>	Disable airtime fairness (ATF) support.	
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable AMSDU support.	
	<i>disable</i>	Disable AMSDU support.	
ap-handoff	Enable/disable AP handoff of clients to other APs (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable AP handoff.	
	<i>disable</i>	Disable AP handoff.	
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size						
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi control frame.								
<i>disable</i>	Disable sniffer on WiFi control frame.								
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi data frame								
<i>disable</i>	Disable sniffer on WiFi data frame								
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management beacon frame.								
<i>disable</i>	Disable sniffer on WiFi management beacon frame.								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management other frame.								
<i>disable</i>	Disable sniffer on WiFi management other frame.								
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management probe frame.								
<i>disable</i>	Enable sniffer on WiFi management probe frame.								
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.		
Option	Description								
<i>enable</i>	Enable automatic transmit power adjustment.								
<i>disable</i>	Disable automatic transmit power adjustment.								
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						
band	WiFi band that Radio 1 operates on.	option	-						

Option	Description
<i>802.11a</i>	802.11a.
<i>802.11b</i>	802.11b.
<i>802.11g</i>	802.11g/b.
<i>802.11n</i>	802.11n/g/b at 2.4GHz.
<i>802.11n-5G</i>	802.11n/a at 5GHz.
<i>802.11ac</i>	802.11ac/n/a.
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.
<i>802.11g-only</i>	802.11g.
<i>802.11n-only</i>	802.11n at 2.4GHz.
<i>802.11n-5G-only</i>	802.11n at 5GHz.
<i>802.11ac,n-only</i>	802.11ac/n.
<i>802.11ac-only</i>	802.11ac.
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.				
	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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.		
	Option	Description									
	5g-full	Full 5G band.									
	5g-high	High 5G band.									
5g-low	Low 5G band.										
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM bandwidth admission control.</td></tr><tr><td>disable</td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	enable	Enable WMM bandwidth admission control.	disable	Disable WMM bandwidth admission control.				
	Option	Description									
	enable	Enable WMM bandwidth admission control.									
disable	Disable WMM bandwidth admission control.										
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000								
beacon-interval	Beacon interval. The time between beacon frames in msec (the actual range of beacon interval depends on the AP platform type, default = 100).	integer	Minimum value: 0 Maximum value: 65535								
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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM call admission control.</td></tr><tr><td>disable</td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	enable	Enable WMM call admission control.	disable	Disable WMM call admission control.				
	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 (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-

Option	Description
<i>160MHz</i>	160 MHz channel width.
<i>80MHz</i>	80 MHz channel width.
<i>40MHz</i>	40 MHz channel width.
<i>20MHz</i>	20 MHz channel width.

channel-utilization	Enable/disable measuring channel utilization.	option	-

Option	Description
<i>enable</i>	Enable measuring channel utilization.
<i>disable</i>	Disable measuring channel utilization.

coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-

Option	Description
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.

darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-

Option	Description
<i>enable</i>	Enable distributed automatic radio resource provisioning.
<i>disable</i>	Disable distributed automatic radio resource provisioning.

Parameter	Description	Type	Size
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346
frequency-handoff	Enable/disable frequency handoff of clients to other channels (default = disable).	option	-
	Option	Description	
	enable	Enable frequency handoff.	
	disable	Disable frequency handoff.	
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 Maximum value: 54000
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.	
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100

Parameter	Description	Type	Size
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-

Option	Description
<i>tim</i>	TIM bit for client in power save mode.
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.
<i>no-11b-rate</i>	Do not send frame using 11b data rate.
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.

protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-

Option	Description
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.
<i>disable</i>	Disable 802.11g protection mode.

rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346

short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-

Option	Description
<i>enable</i>	Select the 400 ns short guard interval (Short GI).
<i>disable</i>	Select the 800 ns long guard interval (Long GI).

spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
<i>enable</i>	Enable spectrum analysis.
<i>disable</i>	Disable spectrum analysis.

Parameter	Description	Type	Size												
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable packet transmission optimization.</td></tr><tr><td>power-save</td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td>aggr-limit</td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td>retry-limit</td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td>send-bar</td><td>Limit transmission of BAR frames.</td></tr></table>	Option	Description	disable	Disable packet transmission optimization.	power-save	Tag client as operating in power save mode if excessive transmit retries occur.	aggr-limit	Set aggregation limit to a lower value when data rate is low.	retry-limit	Set software retry limit to a lower value when data rate is low.	send-bar	Limit transmission of BAR frames.		
Option	Description														
disable	Disable packet transmission optimization.														
power-save	Tag client as operating in power save mode if excessive transmit retries occur.														
aggr-limit	Set aggregation limit to a lower value when data rate is low.														
retry-limit	Set software retry limit to a lower value when data rate is low.														
send-bar	Limit transmission of BAR frames.														
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Automatically select tunnel VAPs.</td></tr><tr><td>disable</td><td>Manually select VAPs.</td></tr></table>	Option	Description	enable	Automatically select tunnel VAPs.	disable	Manually select VAPs.								
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												
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35												
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable zero wait DFS</td></tr><tr><td>disable</td><td>Disable zero wait DFS</td></tr></table>	Option	Description	enable	Enable zero wait DFS	disable	Disable zero wait DFS								
Option	Description														
enable	Enable zero wait DFS														
disable	Disable zero wait DFS														

config radio-2

Parameter	Description	Type	Size
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable airtime fairness (ATF) support.	
	<i>disable</i>	Disable airtime fairness (ATF) support.	
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable AMSDU support.	
	<i>disable</i>	Disable AMSDU support.	
ap-handoff	Enable/disable AP handoff of clients to other APs (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable AP handoff.	
	<i>disable</i>	Disable AP handoff.	
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer on WiFi control frame.	
	<i>disable</i>	Disable sniffer on WiFi control frame.	
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi data frame								
<i>disable</i>	Disable sniffer on WiFi data frame								
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management beacon frame.								
<i>disable</i>	Disable sniffer on WiFi management beacon frame.								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management other frame.								
<i>disable</i>	Disable sniffer on WiFi management other frame.								
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management probe frame.								
<i>disable</i>	Enable sniffer on WiFi management probe frame.								
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.		
Option	Description								
<i>enable</i>	Enable automatic transmit power adjustment.								
<i>disable</i>	Disable automatic transmit power adjustment.								

Parameter	Description	Type	Size
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
band	WiFi band that Radio 2 operates on.	option	-

Option	Description
<i>802.11a</i>	802.11a.
<i>802.11b</i>	802.11b.
<i>802.11g</i>	802.11g/b.
<i>802.11n</i>	802.11n/g/b at 2.4GHz.
<i>802.11n-5G</i>	802.11n/a at 5GHz.
<i>802.11ac</i>	802.11ac/n/a.
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.
<i>802.11g-only</i>	802.11g.
<i>802.11n-only</i>	802.11n at 2.4GHz.
<i>802.11n-5G-only</i>	802.11n at 5GHz.
<i>802.11ac,n-only</i>	802.11ac/n.
<i>802.11ac-only</i>	802.11ac.
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.
<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.
<i>802.11ax-only</i>	802.11ax at 2.4GHz.

band-5g-type	WiFi 5G band type.	option	-

Option	Description
<i>5g-full</i>	Full 5G band.

Parameter	Description	Type	Size
	Option	Description	
	5g-high	High 5G band.	
	5g-low	Low 5G band.	
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-
	Option	Description	
	enable	Enable WMM bandwidth admission control.	
	disable	Disable WMM bandwidth admission control.	
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000
beacon-interval	Beacon interval. The time between beacon frames in msec (the actual range of beacon interval depends on the AP platform type, default = 100).	integer	Minimum value: 0 Maximum value: 65535
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 (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-

Parameter	Description	Type	Size										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>160MHz</td><td>160 MHz channel width.</td></tr><tr><td>80MHz</td><td>80 MHz channel width.</td></tr><tr><td>40MHz</td><td>40 MHz channel width.</td></tr><tr><td>20MHz</td><td>20 MHz channel width.</td></tr></table>	Option	Description	160MHz	160 MHz channel width.	80MHz	80 MHz channel width.	40MHz	40 MHz channel width.	20MHz	20 MHz channel width.		
	Option	Description											
	160MHz	160 MHz channel width.											
	80MHz	80 MHz channel width.											
	40MHz	40 MHz channel width.											
20MHz	20 MHz channel width.												
channel-utilization	Enable/disable measuring channel utilization.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable measuring channel utilization.</td></tr><tr><td>disable</td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	enable	Enable measuring channel utilization.	disable	Disable measuring channel utilization.						
	Option	Description											
	enable	Enable measuring channel utilization.											
disable	Disable measuring channel utilization.												
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td>disable</td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	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.						
	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.												
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td>disable</td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>	Option	Description	enable	Enable distributed automatic radio resource provisioning.	disable	Disable distributed automatic radio resource provisioning.						
	Option	Description											
	enable	Enable distributed automatic radio resource provisioning.											
disable	Disable distributed automatic radio resource provisioning.												
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255										
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346										
frequency-handoff	Enable/disable frequency handoff of clients to other channels (default = disable).	option	-										

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable frequency handoff.
<i>disable</i>	Disable frequency handoff.

max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 Maximum value: 54000
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
<i>disabled</i>	Radio 2 is disabled.
<i>ap</i>	Radio 2 operates as an access point that allows WiFi clients to connect to your network.
<i>monitor</i>	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.
<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.

power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-

Option	Description
<i>tim</i>	TIM bit for client in power save mode.
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.
<i>no-11b-rate</i>	Do not send frame using 11b data rate.
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.

Parameter	Description	Type	Size												
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr><tr><td><i>ctsonly</i></td><td>Enable 802.11g protection CTS only mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11g protection mode.</td></tr></table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.						
Option	Description														
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.														
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.														
<i>disable</i>	Disable 802.11g protection mode.														
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346												
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	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).								
Option	Description														
<i>enable</i>	Select the 400 ns short guard interval (Short GI).														
<i>disable</i>	Select the 800 ns long guard interval (Long GI).														
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable spectrum analysis.</td></tr><tr><td><i>disable</i></td><td>Disable spectrum analysis.</td></tr></table>	Option	Description	<i>enable</i>	Enable spectrum analysis.	<i>disable</i>	Disable spectrum analysis.								
Option	Description														
<i>enable</i>	Enable spectrum analysis.														
<i>disable</i>	Disable spectrum analysis.														
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet transmission optimization.</td></tr><tr><td><i>power-save</i></td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td><i>aggr-limit</i></td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td><i>retry-limit</i></td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td><i>send-bar</i></td><td>Limit transmission of BAR frames.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.		
Option	Description														
<i>disable</i>	Disable packet transmission optimization.														
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.														
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.														
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.														
<i>send-bar</i>	Limit transmission of BAR frames.														

Parameter	Description	Type	Size
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Automatically select tunnel VAPs.	
	<i>disable</i>	Manually select VAPs.	
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable zero wait DFS	
	<i>disable</i>	Disable zero wait DFS	

config radio-3

Parameter	Description	Type	Size						
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.		
Option	Description								
<i>enable</i>	Enable airtime fairness (ATF) support.								
<i>disable</i>	Disable airtime fairness (ATF) support.								
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AMSDU support.</td></tr><tr><td><i>disable</i></td><td>Disable AMSDU support.</td></tr></table>	Option	Description	<i>enable</i>	Enable AMSDU support.	<i>disable</i>	Disable AMSDU support.		
Option	Description								
<i>enable</i>	Enable AMSDU support.								
<i>disable</i>	Disable AMSDU support.								
ap-handoff	Enable/disable AP handoff of clients to other APs (default = disable).	option	-						

Parameter	Description	Type	Size						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP handoff.</td></tr><tr><td><i>disable</i></td><td>Disable AP handoff.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP handoff.	<i>disable</i>	Disable AP handoff.		
Option	Description								
<i>enable</i>	Enable AP handoff.								
<i>disable</i>	Disable AP handoff.								
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified						
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32						
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295						
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi control frame.								
<i>disable</i>	Disable sniffer on WiFi control frame.								
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi data frame								
<i>disable</i>	Disable sniffer on WiFi data frame								
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management beacon frame.								
<i>disable</i>	Disable sniffer on WiFi management beacon frame.								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.				
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management other frame.								

Parameter	Description	Type	Size
	Option	Description	
	<i>disable</i>	Disable sniffer on WiFi management other frame.	
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable sniffer on WiFi management probe frame.	
	<i>disable</i>	Enable sniffer on WiFi management probe frame.	
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable automatic transmit power adjustment.	
	<i>disable</i>	Disable automatic transmit power adjustment.	
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295
band	WiFi band that Radio 3 operates on.	option	-
	Option	Description	
	<i>802.11a</i>	802.11a.	
	<i>802.11b</i>	802.11b.	
	<i>802.11g</i>	802.11g/b.	
	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	
	<i>802.11n-5G</i>	802.11n/a at 5GHz.	
	<i>802.11ac</i>	802.11ac/n/a.	
	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	

Parameter	Description	Type	Size																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11n,g-only</td><td>802.11n/g at 2.4GHz.</td></tr><tr><td>802.11g-only</td><td>802.11g.</td></tr><tr><td>802.11n-only</td><td>802.11n at 2.4GHz.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n at 5GHz.</td></tr><tr><td>802.11ac,n-only</td><td>802.11ac/n.</td></tr><tr><td>802.11ac-only</td><td>802.11ac.</td></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	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.		
	Option	Description																													
	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	-																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.																						
	Option	Description																													
	5g-full	Full 5G band.																													
	5g-high	High 5G band.																													
5g-low	Low 5G band.																														
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM bandwidth admission control.</td></tr><tr><td>disable</td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	enable	Enable WMM bandwidth admission control.	disable	Disable WMM bandwidth admission control.																								
	Option	Description																													
	enable	Enable WMM bandwidth admission control.																													
disable	Disable WMM bandwidth admission control.																														
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000																												

Parameter	Description	Type	Size										
beacon-interval	Beacon interval. The time between beacon frames in msec (the actual range of beacon interval depends on the AP platform type, default = 100).	integer	Minimum value: 0 Maximum value: 65535										
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	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.						
Option	Description												
<i>enable</i>	Enable WMM call admission control.												
<i>disable</i>	Disable WMM call admission control.												
call-capacity	Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60										
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3										
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.		
Option	Description												
<i>160MHz</i>	160 MHz channel width.												
<i>80MHz</i>	80 MHz channel width.												
<i>40MHz</i>	40 MHz channel width.												
<i>20MHz</i>	20 MHz channel width.												
channel-utilization	Enable/disable measuring channel utilization.	option	-										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr><tr><td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.						
Option	Description												
<i>enable</i>	Enable measuring channel utilization.												
<i>disable</i>	Disable measuring channel utilization.												
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-										

Parameter	Description	Type	Size

Option	Description
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.

darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-

Option	Description
<i>enable</i>	Enable distributed automatic radio resource provisioning.
<i>disable</i>	Disable distributed automatic radio resource provisioning.

dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346
frequency-handoff	Enable/disable frequency handoff of clients to other channels (default = disable).	option	-

Option	Description
<i>enable</i>	Enable frequency handoff.
<i>disable</i>	Disable frequency handoff.

max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 Maximum value: 54000
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, or a sniffer.	option	-

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Radio 3 is disabled.</td></tr><tr><td><i>ap</i></td><td>Radio 3 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td><i>monitor</i></td><td>Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr><tr><td><i>sniffer</i></td><td>Radio 3 operates as a sniffer capturing WiFi frames on air.</td></tr></table>	Option	Description	<i>disabled</i>	Radio 3 is disabled.	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.				
	Option	Description													
	<i>disabled</i>	Radio 3 is disabled.													
	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.													
	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.													
<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.														
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100												
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tim</i></td><td>TIM bit for client in power save mode.</td></tr><tr><td><i>ac-vo</i></td><td>Use AC VO priority to send out packets in the power save queue.</td></tr><tr><td><i>no-obss-scan</i></td><td>Do not put OBSS scan IE into beacon and probe response frames.</td></tr><tr><td><i>no-11b-rate</i></td><td>Do not send frame using 11b data rate.</td></tr><tr><td><i>client-rate-follow</i></td><td>Adapt transmitting PHY rate with receiving PHY rate from a client.</td></tr></table>	Option	Description	<i>tim</i>	TIM bit for client in power save mode.	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.	<i>no-11b-rate</i>	Do not send frame using 11b data rate.	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
	Option	Description													
	<i>tim</i>	TIM bit for client in power save mode.													
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.													
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.													
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.													
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.														
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rtscts</i></td><td>Enable 802.11g protection RTS/CTS mode.</td></tr><tr><td><i>ctsonly</i></td><td>Enable 802.11g protection CTS only mode.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11g protection mode.</td></tr></table>	Option	Description	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.	<i>disable</i>	Disable 802.11g protection mode.						
	Option	Description													
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.													
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.													
<i>disable</i>	Disable 802.11g protection mode.														
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346												
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	-												

Parameter	Description	Type	Size												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).								
Option	Description														
<i>enable</i>	Select the 400 ns short guard interval (Short GI).														
<i>disable</i>	Select the 800 ns long guard interval (Long GI).														
spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable spectrum analysis.</td></tr><tr><td><i>disable</i></td><td>Disable spectrum analysis.</td></tr></table>	Option	Description	<i>enable</i>	Enable spectrum analysis.	<i>disable</i>	Disable spectrum analysis.								
Option	Description														
<i>enable</i>	Enable spectrum analysis.														
<i>disable</i>	Disable spectrum analysis.														
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet transmission optimization.</td></tr><tr><td><i>power-save</i></td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td><i>aggr-limit</i></td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td><i>retry-limit</i></td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td><i>send-bar</i></td><td>Limit transmission of BAR frames.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet transmission optimization.	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.	<i>send-bar</i>	Limit transmission of BAR frames.		
Option	Description														
<i>disable</i>	Disable packet transmission optimization.														
<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.														
<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.														
<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.														
<i>send-bar</i>	Limit transmission of BAR frames.														
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Automatically select tunnel VAPs.</td></tr><tr><td><i>disable</i></td><td>Manually select VAPs.</td></tr></table>	Option	Description	<i>enable</i>	Automatically select tunnel VAPs.	<i>disable</i>	Manually select VAPs.								
Option	Description														
<i>enable</i>	Automatically select tunnel VAPs.														
<i>disable</i>	Manually select VAPs.														
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35												
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35												
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-												

Parameter	Description	Type	Size
	Option	Description	
	<i>enable</i>	Enable zero wait DFS	
	<i>disable</i>	Disable zero wait DFS	

config radio-4

Parameter	Description	Type	Size
airtime-fairness	Enable/disable airtime fairness (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable airtime fairness (ATF) support.	
	<i>disable</i>	Disable airtime fairness (ATF) support.	
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients (default = enable).	option	-
	Option	Description	
	<i>enable</i>	Enable AMSDU support.	
	<i>disable</i>	Disable AMSDU support.	
ap-handoff	Enable/disable AP handoff of clients to other APs (default = disable).	option	-
	Option	Description	
	<i>enable</i>	Enable AP handoff.	
	<i>disable</i>	Disable AP handoff.	
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified
ap-sniffer-bufsize	Sniffer buffer size (1 - 32 MB, default = 16).	integer	Minimum value: 1 Maximum value: 32
ap-sniffer-chan	Channel on which to operate the sniffer (default = 6).	integer	Minimum value: 0 Maximum value: 4294967295

Parameter	Description	Type	Size						
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi control frame.								
<i>disable</i>	Disable sniffer on WiFi control frame.								
ap-sniffer-data	Enable/disable sniffer on WiFi data frame (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi data frame								
<i>disable</i>	Disable sniffer on WiFi data frame								
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management beacon frame.	<i>disable</i>	Disable sniffer on WiFi management beacon frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management beacon frame.								
<i>disable</i>	Disable sniffer on WiFi management beacon frame.								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management other frame.								
<i>disable</i>	Disable sniffer on WiFi management other frame.								
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td><i>disable</i></td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management probe frame.	<i>disable</i>	Enable sniffer on WiFi management probe frame.		
Option	Description								
<i>enable</i>	Enable sniffer on WiFi management probe frame.								
<i>disable</i>	Enable sniffer on WiFi management probe frame.								
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-level	Enable/disable automatic power-level adjustment to prevent co-channel interference (default = enable).	option	-						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.		
Option	Description								
<i>enable</i>	Enable automatic transmit power adjustment.								
<i>disable</i>	Disable automatic transmit power adjustment.								
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						
band	WiFi band that Radio 3 operates on.	option	-						

Option	Description
<i>802.11a</i>	802.11a.
<i>802.11b</i>	802.11b.
<i>802.11g</i>	802.11g/b.
<i>802.11n</i>	802.11n/g/b at 2.4GHz.
<i>802.11n-5G</i>	802.11n/a at 5GHz.
<i>802.11ac</i>	802.11ac/n/a.
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.
<i>802.11g-only</i>	802.11g.
<i>802.11n-only</i>	802.11n at 2.4GHz.
<i>802.11n-5G-only</i>	802.11n at 5GHz.
<i>802.11ac,n-only</i>	802.11ac/n.
<i>802.11ac-only</i>	802.11ac.
<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.
<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.
<i>802.11ax-5G-only</i>	802.11ax at 5GHz.
<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.

Parameter	Description	Type	Size								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.				
	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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.		
	Option	Description									
	5g-full	Full 5G band.									
	5g-high	High 5G band.									
5g-low	Low 5G band.										
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM bandwidth admission control.</td></tr><tr><td>disable</td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	enable	Enable WMM bandwidth admission control.	disable	Disable WMM bandwidth admission control.				
	Option	Description									
	enable	Enable WMM bandwidth admission control.									
disable	Disable WMM bandwidth admission control.										
bandwidth-capacity	Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000).	integer	Minimum value: 1 Maximum value: 600000								
beacon-interval	Beacon interval. The time between beacon frames in msec (the actual range of beacon interval depends on the AP platform type, default = 100).	integer	Minimum value: 0 Maximum value: 65535								
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	-								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WMM call admission control.</td></tr><tr><td>disable</td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	enable	Enable WMM call admission control.	disable	Disable WMM call admission control.				
	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 (VoWLAN) phones supported by the radio (0 - 60, default = 10).	integer	Minimum value: 0 Maximum value: 60
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-

Option	Description

<i>160MHz</i>	160 MHz channel width.
<i>80MHz</i>	80 MHz channel width.
<i>40MHz</i>	40 MHz channel width.
<i>20MHz</i>	20 MHz channel width.

channel-utilization	Enable/disable measuring channel utilization.	option	-

Option	Description

<i>enable</i>	Enable measuring channel utilization.
<i>disable</i>	Disable measuring channel utilization.

coexistence	Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).	option	-

Option	Description

<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.

darrp	Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is always using the most optimal channel (default = disable).	option	-

Option	Description

<i>enable</i>	Enable distributed automatic radio resource provisioning.
<i>disable</i>	Disable distributed automatic radio resource provisioning.

Parameter	Description	Type	Size
dtim	Delivery Traffic Indication Map (DTIM) period (1 - 255, default = 1). Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255
frag-threshold	Maximum packet size that can be sent without fragmentation (800 - 2346 bytes, default = 2346).	integer	Minimum value: 800 Maximum value: 2346
frequency-handoff	Enable/disable frequency handoff of clients to other channels (default = disable).	option	-
	Option	Description	
	enable	Enable frequency handoff.	
	disable	Disable frequency handoff.	
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295
max-distance	Maximum expected distance between the AP and clients (0 - 54000 m, default = 0).	integer	Minimum value: 0 Maximum value: 54000
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.	
power-level	Radio power level as a percentage of the maximum transmit power (0 - 100, default = 100).	integer	Minimum value: 0 Maximum value: 100

Parameter	Description	Type	Size
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-

Option	Description
<i>tim</i>	TIM bit for client in power save mode.
<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.
<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.
<i>no-11b-rate</i>	Do not send frame using 11b data rate.
<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.

protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-

Option	Description
<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.
<i>ctsonly</i>	Enable 802.11g protection CTS only mode.
<i>disable</i>	Disable 802.11g protection mode.

rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS (256 - 2346 bytes, default = 2346).	integer	Minimum value: 256 Maximum value: 2346

short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-

Option	Description
<i>enable</i>	Select the 400 ns short guard interval (Short GI).
<i>disable</i>	Select the 800 ns long guard interval (Long GI).

spectrum-analysis	Enable/disable spectrum analysis to find interference that would negatively impact wireless performance.	option	-

Option	Description
<i>enable</i>	Enable spectrum analysis.
<i>disable</i>	Disable spectrum analysis.

Parameter	Description	Type	Size												
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable packet transmission optimization.</td></tr><tr><td>power-save</td><td>Tag client as operating in power save mode if excessive transmit retries occur.</td></tr><tr><td>aggr-limit</td><td>Set aggregation limit to a lower value when data rate is low.</td></tr><tr><td>retry-limit</td><td>Set software retry limit to a lower value when data rate is low.</td></tr><tr><td>send-bar</td><td>Limit transmission of BAR frames.</td></tr></table>	Option	Description	disable	Disable packet transmission optimization.	power-save	Tag client as operating in power save mode if excessive transmit retries occur.	aggr-limit	Set aggregation limit to a lower value when data rate is low.	retry-limit	Set software retry limit to a lower value when data rate is low.	send-bar	Limit transmission of BAR frames.		
Option	Description														
disable	Disable packet transmission optimization.														
power-save	Tag client as operating in power save mode if excessive transmit retries occur.														
aggr-limit	Set aggregation limit to a lower value when data rate is low.														
retry-limit	Set software retry limit to a lower value when data rate is low.														
send-bar	Limit transmission of BAR frames.														
vap-all	Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = enable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Automatically select tunnel VAPs.</td></tr><tr><td>disable</td><td>Manually select VAPs.</td></tr></table>	Option	Description	enable	Automatically select tunnel VAPs.	disable	Manually select VAPs.								
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												
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35												
zero-wait-dfs	Enable/disable zero wait DFS on radio (default = enable).	option	-												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable zero wait DFS</td></tr><tr><td>disable</td><td>Disable zero wait DFS</td></tr></table>	Option	Description	enable	Enable zero wait DFS	disable	Disable zero wait DFS								
Option	Description														
enable	Enable zero wait DFS														
disable	Disable zero wait DFS														

config split-tunneling-acl

Parameter	Description	Type	Size
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295

Included devices

This reference includes commands from the following FortiGate model:

- FortiGate-1000D
- FortiGate-100D
- FortiGate-100EF
- FortiGate-100E
- FortiGate-100F
- FortiGate-101E
- FortiGate-101F
- FortiGate-1100E
- FortiGate-1101E
- FortiGate-1200D
- FortiGate-140D-POE
- FortiGate-140D
- FortiGate-140E-POE
- FortiGate-140E
- FortiGate-1500DT
- FortiGate-1500D
- FortiGate-2000E
- FortiGate-200E
- FortiGate-201E
- FortiGate-2200E
- FortiGate-2201E
- FortiGate-2500E
- FortiGate-3000D
- FortiGate-300D
- FortiGate-300E
- FortiGate-301E
- FortiGate-30E-3G4G-GBL
- FortiGate-30E-3G4G-INTL
- FortiGate-30E-3G4G-NAM
- FortiGate-30E
- FortiGate-3100D
- FortiGate-3200D
- FortiGate-3300E
- FortiGate-3301E
- FortiGate-3400E
- FortiGate-3601E
- FortiGate-3700D
- FortiGate-3800D
- FortiGate-3810D
- FortiGate-3815D
- FortiGate-3960E
- FortiGate-3980E
- FortiGate-400D
- FortiGate-400E-Bypass
- FortiGate-400E
- FortiGate-401E
- FortiGate-40F-3G4G
- FortiGate-40F
- FortiGate-5001D
- FortiGate-5001E1
- FortiGate-5001E
- FortiGate-500D
- FortiGate-500E
- FortiGate-501E
- FortiGate-50E
- FortiGate-51E
- FortiGate-52E
- FortiGate-600D
- FortiGate-600E
- FortiGate-601E
- FortiGate-60E-DSLJ
- FortiGate-60E-DSL
- FortiGate-60E-POE
- FortiGate-60E
- FortiGate-60F
- FortiGate-61E
- FortiGate-61F
- FortiGate-800D
- FortiGate-80E-POE
- FortiGate-80E
- FortiGate-80F
- FortiGate-81E-POE
- FortiGate-81E
- FortiGate-81F-POE
- FortiGate-81F
- FortiGate-900D
- FortiGate-90E
- FortiGate-91E
- FortiGate-92D
- FortiGate-VM64
- FortiGateRugged-30D
- FortiGateRugged-35D
- FortiGateRugged-60F-3G4G
- FortiGateRugged-60F
- FortiGateRugged-90D
- FortiWiFi-30E-3G4G-INTL
- FortiWiFi-30E-3G4G-NAM
- FortiWiFi-30E
- FortiWiFi-40F-3G4G
- FortiWiFi-40F
- FortiWiFi-50E-2R
- FortiWiFi-50E
- FortiWiFi-51E
- FortiWiFi-60E-DSLJ
- FortiWiFi-60E-DSL
- FortiWiFi-60E
- FortiWiFi-60F
- FortiWiFi-61E
- FortiWiFi-61F
- FortiWiFi-80F-2R
- FortiWiFi-81F-2R-POE
- FortiWiFi-81F-2R

- FortiGate-3401E
- FortiGate-3600E
- FortiGate-80F-Bypass
- FortiGate-80F-POE



FORTINET®



Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.