

FortiOS 5.6.2 CLI Reference (Beta)

VERSION 5.6.2



FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



September 21, 2017

FortiOS 5.6.2 CLI Reference (Beta)

01-562-441155-20170921

TABLE OF CONTENTS

Change Log	19
Introduction	20
How this guide is organized.....	20
Availability of commands and options.....	20
Managing Firmware with the FortiGate BIOS	22
Accessing the BIOS.....	22
Navigating the menu.....	22
Loading firmware.....	22
Configuring TFTP parameters.....	23
Initiating TFTP firmware transfer.....	23
Booting the backup firmware.....	24
Using the CLI	25
Connecting to the CLI.....	25
Connecting to the CLI using a local console.....	25
Enabling access to the CLI through the network (SSH or Telnet).....	26
Connecting to the CLI using SSH.....	27
Connecting to the CLI using Telnet.....	28
Command syntax.....	29
Terminology.....	29
Indentation.....	30
Notation.....	30
Sub-commands.....	32
Example of table commands.....	34
Permissions.....	36
Tips.....	36
config	45
alertemail	46
alertemail setting.....	47
antivirus	49
antivirus heuristic.....	50
antivirus profile.....	51
antivirus quarantine.....	59
antivirus settings.....	64

application	65
application custom.....	66
application list.....	68
application name.....	75
application rule-settings.....	77
authentication	78
authentication rule.....	79
authentication scheme.....	82
authentication setting.....	84
aws	85
aws setting.....	86
certificate	87
certificate ca.....	88
certificate crt.....	89
certificate local.....	90
dlp	92
dlp filepattern.....	93
dlp fp-doc-source.....	97
dlp fp-sensitivity.....	101
dlp sensor.....	102
dlp settings.....	108
dnsfilter	110
dnsfilter domain-filter.....	111
dnsfilter profile.....	112
endpoint-control	113
endpoint-control client.....	114
endpoint-control forticlient-registration-sync.....	115
endpoint-control profile.....	116
endpoint-control registered-forticlient.....	121
endpoint-control settings.....	122
extender-controller	123
extender-controller extender.....	124
firewall	126
firewall {acl acl6}.....	128
firewall {address address6}.....	130
firewall {addrgrp addgrp6}.....	143
firewall auth-portal.....	150
firewall central-snat-map.....	151
firewall dnstranslation.....	153
firewall {DoS-policy DoS-policy6}.....	154
firewall identity-based-route.....	157

firewall {interface-policy interface-policy6}.....	158
firewall internet-service.....	161
firewall internet-service-custom.....	162
firewall ipmacbinding setting.....	164
firewall ipmacbinding table.....	165
firewall {ippool ippool6}.....	166
firewall ip-translation.....	168
firewall ipv6-eh-filter.....	169
firewall ldb-monitor.....	170
firewall {local-in-policy local-in-policy6}.....	171
firewall {multicast-address multicast-address6}.....	173
firewall {multicast-policy multicast-policy6}.....	175
firewall {policy policy6}.....	177
firewall {policy46 policy64}.....	225
firewall profile-group.....	228
firewall profile-protocol-options.....	229
firewall proxy-address.....	233
firewall proxy-addrgrp.....	235
firewall proxy-policy.....	236
firewall schedule group.....	240
firewall schedule onetime.....	243
firewall schedule recurring.....	247
firewall service category.....	248
firewall service custom.....	251
firewall service group.....	263
firewall shaper per-ip-shaper.....	264
firewall shaper traffic-shaper.....	265
firewall shaping-policy.....	266
firewall sniffer.....	268
firewall ssl setting.....	270
firewall ssl-server.....	271
firewall ssl-ssh-profile.....	273
firewall ttl-policy.....	278
firewall {vip vip6}.....	279
firewall {vip46 vip64}.....	312
firewall {vipgrp vipgrp6}.....	316
firewall {vipgrp46 vipgrp64}.....	317
ftp-proxy.....	318
ftp-proxy explicit.....	319
icap.....	320
icap profile.....	321
icap server.....	322

ips	323
ips custom.....	324
ips decoder.....	327
ips global.....	328
ips rule.....	332
ips rule-settings.....	335
ips sensor.....	336
ips settings.....	342
log	344
log custom-field.....	346
log disk filter.....	347
log disk setting.....	349
log eventfilter.....	351
log fortianalyzer override-filter.....	353
log fortianalyzer override-setting.....	354
log {fortianalyzer fortianalyzer2 fortianalyzer3} filter.....	356
log {fortianalyzer fortianalyzer2 fortianalyzer3} setting.....	357
log fortiguard filter.....	359
log fortiguard override-filter.....	360
log fortiguard override-setting.....	361
log fortiguard setting.....	362
log gui-display.....	363
log memory filter.....	365
log memory global-setting.....	367
log memory setting.....	368
log null-device filter.....	369
log null-device setting.....	370
log setting.....	371
log syslogd override-filter.....	372
log syslogd override-setting.....	373
log {syslogd syslogd2 syslogd3 syslogd4} filter.....	375
log {syslogd syslogd2 syslogd3 syslogd4} setting.....	376
log threat-weight.....	378
log webtrends filter.....	384
log webtrends setting.....	385
report	386
report chart.....	387
report dataset.....	391
report layout.....	392
report setting.....	396
report style.....	397
report theme.....	399

router	401
router {access-list access-list6}.....	402
router aspath-list.....	404
router auth-path.....	405
router bfd.....	406
router bgp.....	407
router community-list.....	416
router isis.....	417
router key-chain.....	421
router {multicast multicast6}.....	422
router multicast-flow.....	425
router {ospf ospf6}.....	426
router {policy policy6}.....	433
router {prefix-list prefix-list6}.....	435
router rip.....	437
router ripng.....	440
router route-map.....	443
router setting.....	446
router {static static6}.....	447
spamfilter	449
spamfilter bwl.....	450
spamfilter bword.....	451
spamfilter dnsbl.....	453
spamfilter fortishield.....	454
spamfilter iptrust.....	455
spamfilter mheader.....	456
spamfilter options.....	457
spamfilter profile.....	458
switch-controller	460
switch-controller 802-1X-settings.....	461
switch-controller custom-command.....	462
switch-controller global.....	463
switch-controller igmp-snooping.....	464
switch-controller lldp-profile.....	465
switch-controller lldp-settings.....	467
switch-controller mac-sync-settings.....	468
switch-controller managed-switch.....	469
switch-controller qos dot1p-map.....	474
switch-controller qos ip-dscp-map.....	477
switch-controller qos qos-policy.....	479
switch-controller qos queue-policy.....	480
switch-controller quarantine.....	481

switch-controller security-policy 802-1X	482
switch-controller security-policy captive-portal	483
switch-controller storm-control	484
switch-controller stp-settings	485
switch-controller switch-group	486
switch-controller switch-log	487
switch-controller switch-profile	488
switch-controller vlan	489
system	490
system 3g-modem custom	494
system accprofile	495
system admin	499
system alarm	508
system alias	509
system api-user	510
system arp-table	511
system auto-install	512
system auto-script	513
system autoupdate push-update	514
system autoupdate schedule	515
system autoupdate tunneling	516
system central-management	517
system cluster-sync	521
system console	523
system csf	524
system custom-language	526
system ddns	527
system dedicated-mgmt	529
system {dhcp server dhcp6 server}	530
system dns	542
system dns-database	544
system dns-server	546
system dscp-based-priority	547
system email-server	548
system fips-cc	549
system fm	550
system fortiguard	551
system fortimanager	552
system fortisandbox	553
system fsso-polling	554
system ftm-push	555
system geoip-override	556

system global.....	557
system gre-tunnel.....	586
system ha.....	587
system ha-monitor.....	606
system interface.....	607
system ipip-tunnel.....	639
system ips-urlfilter-dns.....	640
system ipv6-neighbor-cache.....	641
system ipv6-tunnel.....	642
system link-monitor.....	643
system lte-modem.....	646
system mac-address-table.....	647
system management-tunnel.....	648
system mobile-tunnel.....	649
system modem.....	650
system nat64.....	653
system netflow.....	654
system network-visibility.....	655
system np6.....	656
system npu.....	665
system ntp.....	668
system object-tag.....	669
system password-policy.....	670
system password-policy-guest-admin.....	673
system physical-switch.....	674
system pppoe-interface.....	675
system probe-response.....	676
system proxy-arp.....	677
system replacemsg admin.....	678
system replacemsg alertmail.....	679
system replacemsg auth.....	680
system replacemsg device-detection-portal.....	681
system replacemsg ec.....	682
system replacemsg fortiguard-wf.....	683
system replacemsg ftp.....	684
system replacemsg http.....	685
system replacemsg mail.....	686
system replacemsg nac-quar.....	687
system replacemsg nntp.....	688
system replacemsg spam.....	689
system replacemsg sslvpn.....	690
system replacemsg traffic-quota.....	691

system replacemsg utm	692
system replacemsg webproxy	693
system replacemsg-group	694
system replacemsg-image	701
system resource-limits	702
system session-helper	703
system session-ttl	704
system settings	705
system sflow	709
system sit-tunnel	710
system sms-server	711
system snmp community	712
system snmp sysinfo	715
system snmp user	716
system storage	718
system stp	719
system switch-interface	720
system tos-based-priority	721
system vdom	722
system vdom-dns	723
system vdom-link	724
system vdom-netflow	725
system vdom-property	726
system vdom-radius-server	727
system vdom-sflow	728
system virtual-switch	729
system virtual-wan-link	730
system virtual-wire-pair	734
system vxlan	735
system wccp	736
Router mode	737
Client mode	739
system wireless ap-status	740
system wireless settings	741
system zone	743
user	744
user adgrp	745
user device	746
user device-access-list	749
user device-category	751
user device-group	752
user fortitoken	753

user fssso.....	755
user fssso-polling.....	757
user group.....	759
user krb-keytab.....	765
user ldap.....	766
user local.....	771
user password-policy.....	775
user peer.....	776
user peergrp.....	779
user pop3.....	780
user radius.....	781
user security-exempt-list.....	793
user setting.....	795
user tacacs+.....	799
voip.....	801
voip profile.....	802
vpn.....	808
vpn certificate ca.....	809
vpn certificate crl.....	811
vpn certificate local.....	814
vpn certificate ocspp-server.....	818
vpn certificate remote.....	820
vpn certificate setting.....	822
vpn ipsec concentrator.....	825
vpn ipsec forticlient.....	826
vpn ipsec {manualkey-interface manualkey}.....	827
vpn ipsec {phase1-interface phase1}.....	835
vpn ipsec {phase2-interface phase2}.....	869
vpn l2tp.....	883
vpn pptp.....	884
vpn ssl settings.....	885
vpn ssl web host-check-software.....	896
vpn ssl web portal.....	899
vpn ssl web realm.....	912
vpn ssl web user-bookmark.....	913
vpn ssl web user-group-bookmark.....	915
vpn ssl web virtual-desktop-app-list.....	921
waf.....	923
waf main-class.....	924
waf profile.....	925
waf signature.....	932
waf sub-class.....	933

wanopt	934
wanopt auth-group.....	935
auth-method {cert psk}.....	935
wanopt forticache-service.....	937
wanopt peer.....	938
wanopt profile.....	939
wanopt settings.....	946
wanopt storage.....	947
wanopt webcache.....	948
webfilter	952
webfilter content.....	953
webfilter content-header.....	954
webfilter cookie-ovrd.....	955
webfilter fortiguard.....	956
webfilter ftgd-local-cat.....	957
webfilter ftgd-local-rating.....	958
webfilter ips-urfilter-cache-setting.....	959
webfilter ips-urfilter-setting.....	960
webfilter override.....	961
webfilter profile.....	962
webfilter search-engine.....	968
webfilter urfilter.....	969
web-proxy	971
web-proxy debug-url.....	972
web-proxy explicit.....	973
web-proxy forward-server.....	979
web-proxy forward-server-group.....	981
web-proxy global.....	983
web-proxy profile.....	986
web-proxy url-match.....	989
web-proxy wisp.....	991
wireless-controller	993
wireless-controller ap-status.....	994
wireless-controller ble-profile.....	995
wireless-controller global.....	996
wireless-controller setting.....	999
wireless-controller timers.....	1003
wireless-controller vap-group.....	1006
wireless-controller wids-profile.....	1007
wireless-controller wtp.....	1014
wireless-controller wtp-group.....	1026
wireless-controller wtp-profile.....	1029

execute	1053
backup	1053
batch	1056
bypass-mode	1057
carrier-license	1057
central-mgmt	1057
cfg reload	1058
cfg save	1059
clear system arp table	1059
cli check-template-status	1059
cli status-msg-only	1060
client-reputation	1060
date	1060
disk	1061
disk raid	1062
disk scan	1063
dhcp lease-clear	1063
dhcp lease-list	1063
disconnect-admin-session	1064
enter	1064
erase-disk	1064
factoryreset	1065
factoryreset2	1065
formatlogdisk	1065
forticarrier-license	1065
forticlient	1065
FortiClient-NAC	1066
fortiguard-log	1066
fortitoken	1067
fortitoken-mobile	1068
fso refresh	1068
ha disconnect	1068
ha ignore-hardware-revision	1069
ha manage	1069
ha synchronize	1070
interface dhcpclient-renew	1071
interface pppoe-reconnect	1071
log backup	1071
log client-reputation-report	1071
log convert-oldlogs	1073
log delete-all	1073
log delete-oldlogs	1073

log detail	1073
log display.....	1074
log downgrade-log.....	1074
log filter.....	1074
log fortianalyzer test-connectivity.....	1075
log list	1076
log rebuild-sqldb.....	1076
log recreate-sqldb.....	1076
log-report reset	1077
log restore.....	1077
log roll.....	1077
log shift-time.....	1077
log upload-progress.....	1078
modem dial.....	1078
modem hangup.....	1078
modem trigger.....	1078
mrouter clear.....	1079
netscan.....	1079
pbx	1080
ping.....	1082
ping-options, ping6-options.....	1082
ping6.....	1084
policy-packet-capture delete-all.....	1084
reboot.....	1084
report.....	1085
report-config reset.....	1085
restore.....	1085
revision.....	1089
router clear bfd session.....	1090
router clear bgp.....	1090
router clear ospf process.....	1091
router restart.....	1091
send-fds-statistics.....	1091
sensor detail.....	1092
sensor list	1092
set system session filter.....	1093
set-next-reboot.....	1095
sfp-mode-sgmii.....	1095
shutdown.....	1095
ssh.....	1096
sync-session.....	1096
system custom-language import.....	1096

system fortisandbox test-connectivity.....	1097
tac report.....	1097
telnet.....	1097
time.....	1097
traceroute.....	1098
tracert6.....	1098
update-av.....	1099
update-geo-ip.....	1099
update-ips.....	1099
update-list.....	1100
update-now.....	1100
update-src-vis.....	1100
upd-vd-license.....	1100
upload.....	1101
usb-device.....	1101
usb-disk.....	1102
vpn certificate ca.....	1102
vpn certificate crl.....	1103
vpn certificate local export.....	1104
vpn certificate local generate.....	1105
vpn certificate local import.....	1107
vpn certificate remote.....	1108
vpn ipsec tunnel down.....	1108
vpn ipsec tunnel up.....	1109
vpn sslvpn del-all.....	1109
vpn sslvpn del-tunnel.....	1109
vpn sslvpn del-web.....	1109
vpn sslvpn list.....	1110
webfilter quota-reset.....	1110
wireless-controller delete-wtp-image.....	1110
wireless-controller list-wtp-image.....	1110
wireless-controller reset-wtp.....	1111
wireless-controller restart-acd.....	1111
wireless-controller restart-wtpd.....	1111
wireless-controller upload-wtp-image.....	1111
get.....	1112
application internet-service status.....	1112
application internet-service-summary.....	1112
certificate.....	1112
extender modem-status.....	1113
extender sys-info.....	1114
firewall dnstranslation.....	1114

firewall iprope appctrl.....	1114
firewall iprope list.....	1114
firewall proute, proute6.....	1115
firewall service custom.....	1115
firewall shaper.....	1116
grep.....	1117
gui console status.....	1117
hardware cpu.....	1118
hardware memory.....	1119
hardware nic.....	1119
hardware npu.....	1120
hardware status.....	1123
ips decoder status.....	1123
ips rule status.....	1124
ips session.....	1124
ips view-map.....	1125
ipsec tunnel.....	1125
mgmt-data status.....	1126
pbx branch-office.....	1126
pbx dialplan.....	1126
pbx did.....	1127
pbx extension.....	1127
pbx ftgd-voice-pkg.....	1127
pbx global.....	1128
pbx ringgrp.....	1128
pbx sip-trunk.....	1129
pbx voice-menu.....	1129
router info bfd neighbor.....	1130
router info bgp.....	1130
router info isis.....	1132
router info kernel.....	1132
router info multicast.....	1133
router info ospf.....	1134
router info protocols.....	1136
router info rip.....	1137
router info routing-table.....	1137
router info vrrp.....	1138
router info6 bgp.....	1138
router info6 interface.....	1139
router info6 kernel.....	1140
router info6 ospf.....	1140
router info6 protocols.....	1140

router info6 rip.....	1140
router info6 routing-table.....	1141
switch-controller poe.....	1141
system admin list.....	1141
system admin status.....	1142
system arp.....	1143
system auto-update.....	1143
system central-management.....	1143
system checksum.....	1144
system cmdb status.....	1144
system fortianalyzer-connectivity.....	1145
system fortiguard-log-service status.....	1145
system fortiguard-service status.....	1146
system ha-nonsync-csum.....	1146
system ha status.....	1146
system info admin status.....	1149
system info admin ssh.....	1150
system interface physical.....	1150
system ip-conflict status.....	1151
system mgmt-csum.....	1151
system performance firewall.....	1151
system performance status.....	1152
system performance top.....	1153
system session list.....	1154
system session status.....	1155
system session-helper-info list.....	1155
system session-info.....	1156
system source-ip.....	1157
system startup-error-log.....	1158
system stp list.....	1158
system status.....	1158
test.....	1159
user adgrp.....	1161
vpn certificate.....	1161
vpn ike gateway.....	1162
vpn ipsec tunnel details.....	1162
vpn ipsec tunnel name.....	1162
vpn ipsec tunnel summary.....	1162
vpn ipsec stats crypto.....	1162
vpn ipsec stats tunnel.....	1163
vpn ssl monitor.....	1163
vpn status l2tp.....	1164

vpn status pptp.....	1164
vpn status ssl.....	1164
webfilter categories.....	1164
webfilter ftgd-statistics.....	1165
webfilter status.....	1167
wireless-controller client-info.....	1167
wireless-controller rf-analysis.....	1167
wireless-controller scan.....	1168
wireless-controller spectral-info.....	1168
wireless-controller status.....	1169
wireless-controller vap-status.....	1169
wireless-controller wlchanlistlic.....	1169
wireless-controller wtp-status.....	1171
tree.....	1173

Change Log

Date	Change Description
September 21, 2017	Beta release.

Introduction

This document describes FortiOS 5.6 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI).

Beta release

This document is released as a Beta and, as such, is very much a work in progress. Before now, our focus was on documenting the most commonly used CLI commands, or those commands that required more explanation. Now we are releasing this Beta with every possible command available, with Supplemental Information below the CLI syntax that dive into a little extra detail.

The CLI syntax is created by processing a schema of a particular build of FortiOS 5.6, and reformatting the resulting CLI output into content that resembles the output found in the CLI console.

In addition, we will continue to improve the supplemental information, and have an HTML version up soon accessible from <http://cli.fortinet.com>.

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

How this guide is organized

This document contains the following sections:

[Managing Firmware with the FortiGate BIOS](#) describes how to change firmware at the console during FortiGate unit boot-up.

[Using the CLI](#) describes how to connect to the CLI and some basics of how it works.

[config](#) describes the commands for each configuration branch of the FortiOS CLI.

[execute](#) describes execute commands.

[get](#) describes get commands.

[tree](#) describes the tree command.

Availability of commands and options

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

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

FortiGate model

All commands are not available on all FortiGate models. For example, low-end FortiGate models do not support the aggregate interface type option of the `config system interface` command.

Hardware configuration

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

FortiOS Carrier, FortiGate Voice, FortiWiFi, etc

Commands for extended functionality are not available on all FortiGate models. The CLI Reference includes commands only available for FortiWiFi units, FortiOS Carrier, and FortiGate Voice units.

Managing Firmware with the FortiGate BIOS

FortiGate units are shipped with firmware installed. Usually firmware upgrades are performed through the web-based manager or by using the CLI `execute restore` command. From the console, you can also interrupt the FortiGate unit's boot-up process to load firmware using the BIOS firmware that is a permanent part of the unit.

Using the BIOS, you can:

- view system information
- format the boot device
- load firmware and reboot
- reboot the FortiGate unit from the backup firmware, which then becomes the default firmware

Accessing the BIOS

The BIOS menu is available only through direct connection to the FortiGate unit's Console port. During boot-up, "Press any key" appears briefly. If you press any keyboard key at this time, boot-up is suspended and the BIOS menu appears. If you are too late, the boot-up process continues as usual.

Navigating the menu

The main BIOS menu looks like this:

```
[C]: Configure TFTP parameters
[R]: Review TFTP paramters
[T]: Initiate TFTP firmware transfer
[F]: Format boot device
[Q]: Quit menu and continue to boot
[I]: System Information
[B]: Boot with backup firmare and set as default
[Q]: Quit menu and continue to boot
[H]: Display this list of options
```

Enter C,R,T,F,I,B,Q, or H:

Typing the bracketed letter selects the option. Input is case-sensitive. Most options present a submenu. An option value in square brackets at the end of the "Enter" line is the default value which you can enter simply by pressing Return. For example,

```
Enter image download port number [WAN1]:
```

In most menus, typing H re-lists the menu options and typing Q returns to the previous menu.

Loading firmware

The BIOS can download firmware from a TFTP server that is reachable from a FortiGate unit network interface. You need to know the IP address of the server and the name of the firmware file to download.

The downloaded firmware can be saved as either the default or backup firmware. It is also possible to boot the downloaded firmware without saving it.

Configuring TFTP parameters

Starting from the main BIOS menu

```
[C]: Configure TFTP parameters.
```

Selecting the VLAN (if VLANs are used)

```
[V]: Set local VLAN ID.
```

Choose port and whether to use DHCP

```
[P]: Set firmware download port.
```

The options listed depend on the FortiGate model. Choose the network interface through which the TFTP server can be reached. For example:

```
[0]: Any of port 1 - 7
[1]: WAN1
[2]: WAN2
Enter image download port number [WAN1]:
[D]: Set DHCP mode.
Please select DHCP setting
[1]: Enable DHCP
[2]: Disable DHCP
```

If there is a DHCP server on the network, select [1]. This simplifies configuration. Otherwise, select [2].

Non-DHCP steps

```
[I]: Set local IP address.
Enter local IP address [192.168.1.188]:
```

This is a temporary IP address for the FortiGate unit network interface. Use a unique address on the same subnet to which the network interface connects.

```
[S]: Set local subnet mask.
Enter local subnet mask [255.255.252.0]:
[G]: Set local gateway.
```

The local gateway IP address is needed if the TFTP server is on a different subnet than the one to which the FortiGate unit is connected.

TFTP and filename

```
[T]: Set remote TFTP server IP address.
Enter remote TFTP server IP address [192.168.1.145]:
[F]: Set firmware file name.
Enter firmware file name [image.out]:
```

Enter [Q] to return to the main menu.

Initiating TFTP firmware transfer

Starting from the main BIOS menu

```
[T]: Initiate TFTP firmware transfer.
```

```

Please connect TFTP server to Ethernet port 'WAN1'.

MAC: 00:09:0f:b5:55:28

Connect to tftp server 192.168.1.145 ...

#####
Image Received.
Checking image... OK
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
    
```

After you choose any option, the FortiGate unit reboots. If you choose [D] or [B], there is first a pause while the firmware is copied:

```

Programming the boot device now.
.....
.....
    
```

Booting the backup firmware

You can reboot the FortiGate unit from the backup firmware, which then becomes the default firmware.

Starting from the main BIOS menu

```
[B]: Boot with backup firmware and set as default.
```

If the boot device contains backup firmware, the FortiGate unit reboots. Otherwise the unit responds:

```

Failed to mount filesystem. . .
Mount back up partition failed.
Back up image open failed.
Press 'Y' or 'y' to boot default image.
    
```


Using the CLI

The command line interface (CLI) is an alternative configuration tool to the GUI or web-based manager. While the configuration of the GUI uses a point-and-click method, the CLI requires typing commands or uploading batches of commands from a text file, like a configuration script.

This section explains common CLI tasks that an administrator does on a regular basis and includes the topics:

- [Connecting to the CLI](#)
- [Command syntax](#)
- [Sub-commands](#)
- [Permissions](#)
- [Tips](#)

Connecting to the CLI

You can access the CLI in three ways:

- [Locally with a console cable](#) — Connect your computer directly to the FortiGate unit's console port. Local access is required in some cases:
 - If you are installing your FortiGate unit for the first time and it is not yet configured to connect to your network, you may only be able to connect to the CLI using a local serial console connection, unless you reconfigure your computer's network settings for a peer connection.
 - Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until after the boot process has completed, making local CLI access the only viable option.
- [Through the network](#) — Connect your computer through any network attached to one of the FortiGate unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect by accessing the **CLI Console** in the GUI. The CLI console widget is no longer part of the **Dashboard** with FortiOS 5.6. It can be accessed, however, from the upper-right hand corner of the screen and is no longer a pop-out window but a sliding window.
- [Locally with FortiExplorer](#) — Connect your computer directly to the FortiGate unit's USB management port. FortiExplorer provides direct access to the FortiOS setup wizard, Web-based Manager, and CLI console.

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port. To connect to the local console you need:

- A computer with an available serial communications (COM) port.
- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package.
- Terminal emulation software such as HyperTerminal for Microsoft Windows.

The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start HyperTerminal.
3. For the **Connection Description**, enter a **Name** for the connection, and select **OK**.
4. On the **Connect using** drop-down list box, select the communications (COM) port on your management computer you are using to connect to the FortiGate unit.
5. Select **OK**.
6. Select the following **Port** settings and select **OK**.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press **Enter** or **Return** on your keyboard to connect to the CLI.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

The CLI displays the following text:

```
Welcome!
Type ? to list available commands.
```

You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI is accomplished by connecting your computer to the FortiGate unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.



If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the **CLI Console** widget in the web-based manager.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is not connected directly or through a switch, you must also configure the FortiGate unit with a static route to a router that can forward packets from the FortiGate unit to your computer. You can do this using either a local console connection or the web-based manager.

Requirements

- A computer with an available serial communications (COM) port and RJ-45 port
- Terminal emulation software such as HyperTerminal for Microsoft Windows

- The RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- A network cable
- Prior configuration of the operating mode, network interface, and static route.

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiGate unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI.
4. Enter the following command:

```
config system interface
  edit <interface_str>
    set allowaccess <protocols_list>
  end
```

where:

- <interface_str> is the name of the network interface associated with the physical network port and containing its number, such as `port1`
- <protocols_list> is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
config system interface
  edit port1
    set allowaccess ssh telnet
  end
```

5. To confirm the configuration, enter the command to display the network interface's settings.

```
show system interface <interface_str>
```

The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

Connecting to the CLI using SSH

Once the FortiGate unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. FortiGate units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1. On your management computer, start an SSH client.
2. In **Host Name (or IP Address)**, enter the IP address of a network interface on which you have enabled SSH administrative access.
3. In **Port**, enter `22`.

4. For the **Connection type**, select **SSH**.

5. Select **Open**.

The SSH client connects to the FortiGate unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiGate unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiGate unit but used a different IP address or SSH key. This is normal. If your management computer is directly connected to the FortiGate unit with no network hosts between them.

6. Click **Yes** to verify the fingerprint and accept the FortiGate unit's SSH key. You will not be able to log in until you have accepted the key.
7. The CLI displays a login prompt.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for this administrator account and press Enter.

The FortiGate unit displays a command prompt (its host name followed by a #). You can now enter CLI commands.



If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Connecting to the CLI using Telnet

Once the FortiGate unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.



Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept Telnet connections.

To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiGate network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.
4. Type the password for this administrator account and press Enter.

The FortiGate unit displays a command prompt (its host name followed by a #). You can now enter CLI commands.



If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the conventions below to describe valid command syntax.

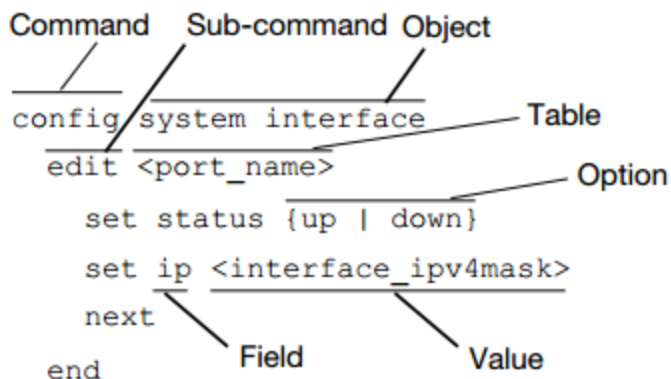
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiGate unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multiline command lines, which can be entered using an escape sequence. Valid command lines must be unambiguous if abbreviated. Optional words or other command line permutations are indicated by syntax notation.
- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands. Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope.
- **object** — A part of the configuration that contains tables and / or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them.

- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiGate unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation.
- **option** — A kind of value that must be one or more words from of a fixed set of options.

Indentation

Indentation indicates levels of nested commands, which indicate what other sub-commands are available from within the scope. For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
  end
```

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Command syntax notation

Convention	Description
Square brackets []	<p>A non-required word or series of words. For example:</p> <pre>[verbose {1 2 3}]</pre> <p>indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as <code>verbose 3</code>.</p>

Convention	Description
<p>Angle brackets < ></p>	<p>A word constrained by data type. The angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example, <retries_int>, indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> • <xxx_name>: A name referring to another part of the configuration, such as policy_A. • <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as *@example.com to match all email addresses ending in @example.com. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as mail.example.com. • <xxx_email>: An email address, such as admin@example.com. • <xxx_ipv4>: An IPv4 address, such as 192.168.1.99. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as 255.255.255.0. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.1/24 • <xxx_ipv4range> : A hyphen (-)-delimited inclusive range of IPv4 addresses, such as 192.168.1.1-192.168.1.255. • <xxx_ipv6>: A colon (:)-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234. • <xxx_v6mask>: An IPv6 netmask, such as /96. • <xxx_ipv6mask>: A dotted decimal IPv6 address and netmask separated by a space. • <xxx_str>: A string of characters that is not another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. • <xxx_int>: An integer number that is not another data type, such as 15 for the number of minutes.
<p>Curly braces { }</p>	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [].</p>

Convention	Description
Options delimited by vertical bars 	<p>Mutually exclusive options. For example:</p> <pre>{enable disable}</pre> <p>indicates that you must enter either <code>enable</code> or <code>disable</code>, but must not enter both.</p>
Options delimited by spaces	<p>Non-mutually exclusive options. For example:</p> <pre>{http https ping snmp ssh telnet}</pre> <p>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:</p> <pre>ping https ssh</pre>

Sub-commands

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands. When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
  next
end
```

Sub-command scope is indicated by indentation.

Available sub-commands vary by command. From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

Commands for tables

clone <table>

Clone (or make a copy of) a table from the current object.

For example, in `config firewall policy`, you could enter the following command to clone security policy 27 to create security policy 30:

```
clone 27 to 30
```

In `config antivirus profile`, you could enter the following command to clone an antivirus profile named `av_pro_1` to create a new antivirus profile named `av_pro_2`:

```
clone av_pro_1 to av_pro_2
```

`clone` may not be available for all tables.

delete <table>

Remove a table from the current object.

For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s first-name and email-address.

`delete` is only available within objects containing tables.

edit <table>

Create or edit a table in the current object.

For example, in `config system admin`:

- edit the settings for the default `admin` administrator account by typing `edit admin`.
- add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`.

`edit` is an interactive sub-command: further sub-commands are available from within `edit`.

`edit` changes the prompt to reflect the table you are currently editing.

`edit` is only available within objects containing tables.

In objects such as security policies, `<table>` is a sequence number. To create a new entry without the risk of overwriting an existing one, enter `edit 0`. The CLI initially confirms the creation of entry 0, but assigns the next unused number after you finish editing and enter `end`.

end

Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.

get	<p>List the configuration of the current object or table.</p> <ul style="list-style-type: none"> • In objects, <code>get</code> lists the table names (if present), or fields and their values. • In a table, <code>get</code> lists the fields and their values. <p>For more information on <code>get</code> commands, see the CLI Reference.</p>
purge	<p>Remove all tables in the current object.</p> <p>For example, in <code>config user local</code>, you could type <code>get</code> to see the list of user names, then type <code>purge</code> and then <code>y</code> to confirm that you want to delete all users.</p> <p><code>purge</code> is only available for objects containing tables.</p> <p>Caution: Back up the FortiGate before performing a <code>purge</code>. <code>purge</code> cannot be undone. To restore purged tables, the configuration must be restored from a backup.</p> <p>Caution: Do not <code>purge system interface</code> or <code>system admin</code> tables. <code>purge</code> does not provide default tables. This can result in being unable to connect or log in, requiring the FortiGate unit to be formatted and restored.</p>
rename <table> to <table>	<p>Rename a table.</p> <p>For example, in <code>config system admin</code>, you could rename <code>admin3</code> to <code>fwadmin</code> by typing <code>rename admin3 to fwadmin</code>.</p> <p><code>rename</code> is only available within objects containing tables.</p>
show	<p>Display changes to the default configuration. Changes are listed in the form of configuration commands.</p>

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Commands for fields

abort	Exit both the <code>edit</code> and/or <code>config</code> commands without saving the fields.
--------------	--

append	Add an option to an existing list.
end	Save the changes made to the current table or object fields, and exit the <code>config</code> command. (To exit without saving, use <code>abort</code> instead.)
get	List the configuration of the current object or table. <ul style="list-style-type: none"> • In objects, <code>get</code> lists the table names (if present), or fields and their values. • In a table, <code>get</code> lists the fields and their values.
move	Move an object within a list, when list order is important. For example, rearranging security policies within the policy list.
next	Save the changes you have made in the current table's fields, and exit the <code>edit</code> command to the object prompt. (To save and exit completely to the root prompt, use <code>end</code> instead.) <p><code>next</code> is useful when you want to create or edit several tables in the same object, without leaving and re-entering the <code>config</code> command each time.</p> <p><code>next</code> is only available from a table prompt; it is not available from an object prompt.</p>
select	Clear all options except for those specified. <p>For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command <code>select member B</code>.</p>
set <field> <value>	Set a field's value. <p>For example, in <code>config system admin</code>, after typing <code>edit admin</code>, you could type <code>set password newpass</code> to change the password of the <code>admin</code> administrator to <code>newpass</code>.</p> <p>Note: When using <code>set</code> to change a field containing a space-delimited list, type the whole new list. For example, <code>set <field> <new-value></code> will replace the list with the <code><new-value></code> rather than appending <code><new-value></code> to the list.</p>
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unselect	Remove an option from an existing list.
unset <field>	Reset the table or object's fields to default values. <p>For example, in <code>config system admin</code>, after typing <code>edit admin</code>, typing <code>unset password</code> resets the password of the <code>admin</code> administrator account to the default (in this case, no password).</p>

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Access profiles control which CLI commands an administrator account can access. Access profiles assign either read, write, or no access to each area of the FortiGate software. To view configurations, you must have read access. To make changes, you must have write access. So, depending on the account used to log in to the FortiGate unit, you may not have complete access to all CLI commands

Unlike other administrator accounts, the `admin` administrator account exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing **all** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.



Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiGate unit.

For complete access to all commands, you must log in with the administrator account named `admin`.

Tips

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words.	?
If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	
Complete the word with the next available match.	Tab
Press the key multiple times to cycle through available matches.	
Recall the previous command.	Up arrow, or Ctrl + P
Command memory is limited to the current session.	
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines.	Ctrl + C
If you are not currently within an interactive command such as <code>config</code> or <code>edit</code> , this closes the CLI connection.	
Continue typing a command on the next line for a multi-line command.	
For each line that you want to continue, terminate it with a backslash (<code>\</code>). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	<code>\</code> then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy stat`.

Adding and removing options from lists

When adding options to a list, such as a user group, using the `set` command will remove the previous configuration. For example, if you wish to add user D to a user group that already contains members A, B, and C, the command would need to be `set member A B C D`. If only `set member D` was used, then all former members would be removed from the group.

However, there are additional commands which can be used instead of `set` for changing options in a list.

Additional commands for lists

append	Add an option to an existing list. For example, <code>append member</code> would add user D to a user group while all previous group members are retained
select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command <code>select member B</code> .
unselect	Remove an option from an existing list. For example, <code>unselect member A</code> would remove member A from a group while all previous group members are retained.

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

Environment variables

\$USERFROM	The management access type (<code>ssh</code> , <code>telnet</code> , <code>jsconsole</code> for the CLI Console widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
\$USERNAME	The account name of the administrator that configured the item.
\$SerialNum	The serial number of the FortiGate unit.

For example, the FortiGate unit's host name can be set to its serial number.

```
config system global
    set hostname $SerialNum
end
```

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields. These characters are special characters, also known as reserved characters.

You may be able to enter special character as part of a string's value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\) character.

In other cases, different keystrokes are required to input a special character. If you need to enter ? as part of config, you first need to input CTRL-V. If you enter the question mark (?) without first using CTRL-V, the question mark has a different meaning in CLI: it will show available command options in that section.

For example, if you enter ? without CTRL-V:

```
edit "*.xe
token line: Unmatched double quote.
```

If you enter ? with CTRL-V:

```
edit "*.xe?"
new entry '*.xe?' added
```

Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	<p>Enclose the string in quotation marks: "Security Administrator".</p> <p>Enclose the string in single quotes: 'Security Administrator'.</p> <p>Precede the space with a backslash: Security\ Administrator.</p>
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Using grep to filter get and show command output

In many cases, the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large `get` or `show` command output, you can use the `grep` command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX `grep`, used for searching text output based on regular expressions.

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr           00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
```

Use the following command to display all lines in HTTP replacement message commands that contain URL (upper or lower case):

```
show system replacemsg http | grep -i url
```

There are three additional options that can be applied to `grep`:

```
-A <num> After
-B <num> Before
-C <num> Context
```

The option `-f` is also available to support Fortinet contextual output, in order to show the complete configuration. The following example shows the difference in output when `-f` option is used versus when it is not.

Using -f:

```
show | grep -f ldap-group1
config user group
  edit "ldap-group1"
    set member "pc40-LDAP"
  next
end
config firewall policy
  edit 2
    set srcintf "port31"
    set dstintf "port32"
    set srcaddr "all"
    set action accept
    set identity-based enable
    set nat enable
  config identity-based-policy
    edit 1
      set schedule "always"
      set groups "ldap-group1"
      set dstaddr "all"
      set service "ALL"
    next
  end
next
end
```


Without using -f:

```
show | grep ldap-group1
edit "ldap-group1"
set groups "ldap-group1"
```

Language support and regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice. To use other languages in those cases, you must use the correct encoding.

Input is stored using Unicode UTF-8 encoding but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes (\) could be inadvertently interpreted as the symbol for the Japanese yen (¥) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.



HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

If you configure your FortiGate unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

If you choose to configure parts of the FortiGate unit using non-ASCII characters, verify that all systems interacting with the FortiGate unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

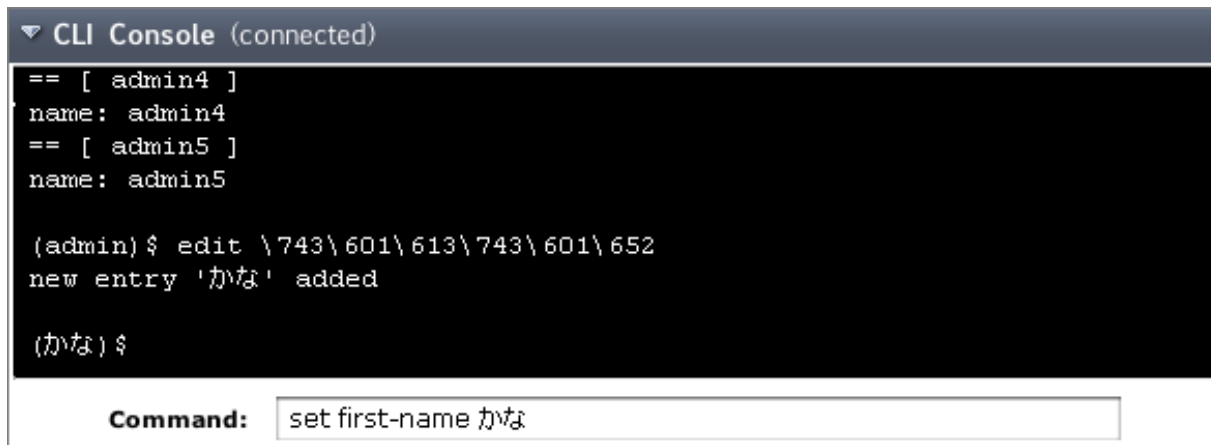
Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the GUI or CLI. Exceptions include items such as

regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiGate unit receives.

To enter non-ASCII characters in the CLI Console

1. On your management computer, start your web browser and go to the URL for the FortiGate unit's GUI.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiGate unit.
4. Open the CLI Console from the upper right-hand corner.
5. In title bar of the **CLI Console** widget, click **Edit** (the pencil icon).
6. Enable **Use external command input box**.
7. Select **OK**.
8. The **Command** field appears below the usual input and display area of the **CLI Console**.
9. In **Command**, type a command.

Entering encoded characters (CLI Console widget):



```

CLI Console (connected)
== [ admin4 ]
name: admin4
== [ admin5 ]
name: admin5

(admin)$ edit \743\601\613\743\601\652
new entry 'かな' added

(かな)$

Command: set first-name かな

```

10. Press **Enter**.

In the display area, the **CLI Console** widget displays your previous command interpreted into its character code equivalent, such as:

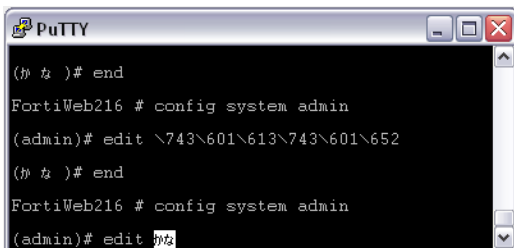
```
edit \743\601\613\743\601\652
```

and the command's output.

To enter non-ASCII characters in a Telnet/SSH client

1. On your management computer, start your Telnet or SSH client.
2. Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding.
Support for sending and receiving international characters varies by each Telnet/SSH client. Consult the documentation for your Telnet/SSH client.
3. Log in to the FortiGate unit.
4. At the command prompt, type your command and press Enter.

Entering encoded characters (PuTTY):



You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet/SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5. The CLI displays your previous command and its output.

Screen paging

You can configure the CLI to pause after displaying each page's worth of text when displaying multiple pages of output. When the display pauses, the last line displays `--More--`. You can then either:

- press the spacebar to display the next page.
- type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
  set output more
end
```

Baud rate

You can change the default baud rate of the local console connection.

To change the baud rate enter the following commands:

```
config system console
  set baudrate {115200 | 19200 | 38400 | 57600 | 9600}
end
```

Editing the configuration file on an external host

You can edit the FortiGate configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiGate unit.

Editing the configuration on an external host can be timesaving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1. Use `execute backup` to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.



Do not edit the first line. The first line(s) of the configuration file (preceded by a # character) contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration file when you attempt to restore it.

3. Use `execute restore` to upload the modified configuration file back to the FortiGate unit. The FortiGate unit downloads the configuration file and checks that the model information is correct. If it is, the FortiGate unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiGate unit ignores the command. If the configuration file is valid, the FortiGate unit restarts and loads the new configuration.

config

Use the config commands to change your FortiGate's configuration.

The command branches and commands are in alphabetical order. The information in this section has been extracted and formatted from FortiOS source code. The extracted information includes the command syntax, command descriptions (extracted from CLI help) and default values. This is the first version of this content produced in this way. You can send comments about this content to techdoc@fortinet.com

alertemail

Use the alert email command to configure various alert email settings.

This section includes syntax for the following commands:

- [alertemail setting](#)

alertemail setting

Configure alert email settings, including destination email addresses and various logging options.

```

config alertemail setting
  set username { string } Name that appears in the From: field of alert emails (max. 36 characters). size[35]
  set mailto1 { string } Email address to send alert email to (usually a system administrator) (max. 64 characters). size[63]
  set mailto2 { string } Optional second email address to send alert email to (max. 64 characters). size[63]
  set mailto3 { string } Optional third email address to send alert email to (max. 64 characters). size[63]
  set filter-mode { category | threshold } How to filter log messages that are sent to alert emails.
    category Filter based on category.
    threshold Filter based on severity.
  set email-interval { integer } Interval between sending alert emails (1 - 99999 min, default = 5). range[1-99999]
  set IPS-logs { enable | disable } Enable/disable IPS logs in alert email.
  set firewall-authentication-failure-logs { enable | disable } Enable/disable firewall authentication failure logs in alert email.
  set HA-logs { enable | disable } Enable/disable HA logs in alert email.
  set IPsec-errors-logs { enable | disable } Enable/disable IPsec error logs in alert email.
  set FDS-update-logs { enable | disable } Enable/disable FortiGuard update logs in alert email.
  set PPP-errors-logs { enable | disable } Enable/disable PPP error logs in alert email.
  set sslvpn-authentication-errors-logs { enable | disable } Enable/disable SSL-VPN authentication error logs in alert email.
  set antivirus-logs { enable | disable } Enable/disable antivirus logs in alert email.
  set webfilter-logs { enable | disable } Enable/disable web filter logs in alert email.
  set configuration-changes-logs { enable | disable } Enable/disable configuration change logs in alert email.
  set violation-traffic-logs { enable | disable } Enable/disable violation traffic logs in alert email.
  set admin-login-logs { enable | disable } Enable/disable administrator login/logout logs in alert email.
  set FDS-license-expiring-warning { enable | disable } Enable/disable FortiGuard license expiration warnings in alert email.
  set log-disk-usage-warning { enable | disable } Enable/disable disk usage warnings in alert email.
  set fortiguard-log-quota-warning { enable | disable } Enable/disable FortiCloud log quota warnings in alert email.
  set amc-interface-bypass-mode { enable | disable } Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert
email.
  set FIPS-CC-errors { enable | disable } Enable/disable FIPS and Common Criteria error logs in alert email.
  set FSSO-disconnect-logs { enable | disable } Enable/disable logging of FSSO collector agent disconnect.
  set FDS-license-expiring-days { integer } Number of days to send alert email prior to FortiGuard license expiration (1 - 100 days, default =
100). range[1-100]
  set local-disk-usage { integer } Disk usage percentage at which to send alert email (1 - 99 percent, default = 75). range[1-99]
  set emergency-interval { integer } Emergency alert interval in minutes. range[1-99999]
  set alert-interval { integer } Alert alert interval in minutes. range[1-99999]
  set critical-interval { integer } Critical alert interval in minutes. range[1-99999]
  set error-interval { integer } Error alert interval in minutes. range[1-99999]

```

```
set warning-interval { integer } Warning alert interval in minutes. range[1-99999]
set notification-interval { integer } Notification alert interval in minutes. range[1-99999]
set information-interval { integer } Information alert interval in minutes. range[1-99999]
set debug-interval { integer } Debug alert interval in minutes. range[1-99999]
set severity { option } Lowest severity level to log.
    emergency    Emergency level.
    alert        Alert level.
    critical     Critical level.
    error        Error level.
    warning      Warning level.
    notification Notification level.
    information  Information level.
    debug        Debug level.

end
```


antivirus

Use antivirus commands to configure antivirus scanning for services, quarantine options, and to enable or disable grayware and heuristic scanning.

This section includes syntax for the following commands:

- [antivirus heuristic](#)
- [antivirus profile](#)
- [antivirus quarantine](#)
- [antivirus settings](#)

antivirus heuristic

Configure the global heuristic options used for antivirus scanning.

```
config antivirus heuristic
  set mode { pass | block | disable }  Enable/disable heuristics and determine how the system behaves if heuristics detects a problem.
  pass      Enable heuristics but detected files are passed. If enabled, the system will record a log message.
  block     Enable heuristics and detected files are blocked. If enabled, the system will record a log message.
  disable   Turn off heuristics.
end
```

antivirus profile

Create and configure antivirus profiles that can be applied to firewall policies.

```

config antivirus profile
  edit { name }
  # Configure AntiVirus profiles.
  set name { string } Profile name. size[35]
  set comment { string } Comment. size[255]
  set replacemsg-group { string } Replacement message group customized for this profile. size[35] - datasource(s): system.replacemsg-group.-
name
  set inspection-mode { proxy | flow-based } Inspection mode.
    proxy Proxy-based inspection.
    flow-based Flow-based inspection.
  set ftgd-analytics { disable | suspicious | everything } Settings to control which files are uploaded to FortiSandbox.
    disable Do not upload files to FortiSandbox.
    suspicious Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.
    everything Submit all files scanned by AntiVirus to FortiSandbox. AntiVirus may not scan all files.
  set analytics-max-upload { integer } Maximum size of files that can be uploaded to FortiSandbox (1 - 395 MBytes, default = 10). range[1-
1606]
  set analytics-wl-filetype { integer } Do not submit files matching this DLP file-pattern to FortiSandbox. range[0-4294967295] - datasource
(s): dlp.filepattern.id
  set analytics-bl-filetype { integer } Only submit files matching this DLP file-pattern to FortiSandbox. range[0-4294967295] - datasource
(s): dlp.filepattern.id
  set analytics-db { disable | enable } Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.
  set mobile-malware-db { disable | enable } Enable/disable using the mobile malware signature database.
  set options { scan | avmonitor | quarantine } Enable/disable HTTP AntiVirus scanning, monitoring, and quarantine.
    scan Enable HTTP antivirus scanning.
    avmonitor Enable HTTP antivirus logging.
    quarantine Enable HTTP antivirus quarantine. Files are quarantined depending on quarantine settings.
  set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested Block nested archives.
    mailbomb Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
  set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.

```

```
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested    Log nested archives.
    mailbomb  Log mail bomb archives.
    unhandled Log archives that FortiOS cannot open.
set emulator { enable | disable } Enable/disable the virus emulator.
set options { scan | avmonitor | quarantine } Enable/disable FTP AntiVirus scanning, monitoring, and quarantine.
    scan      Enable FTP antivirus scanning.
    avmonitor Enable FTP antivirus logging.
    quarantine Enable FTP antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested    Block nested archives.
    mailbomb  Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested    Log nested archives.
    mailbomb  Log mail bomb archives.
    unhandled Log archives that FortiOS cannot open.
set emulator { enable | disable } Enable/disable the virus emulator.
set options { scan | avmonitor | quarantine } Enable/disable IMAP AntiVirus scanning, monitoring, and quarantine.
    scan      Enable IMAP antivirus scanning.
    avmonitor Enable IMAP antivirus logging.
    quarantine Enable IMAP antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested    Block nested archives.
    mailbomb  Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested    Log nested archives.
    mailbomb  Log mail bomb archives.
    unhandled Log archives that FortiOS cannot open.
```

```
set emulator { enable | disable } Enable/disable the virus emulator.
set executables { default | virus } Treat Windows executable files as viruses for the purpose of blocking or monitoring.
    default Perform standard AntiVirus scanning of Windows executable files.
    virus Treat Windows executables as viruses.
set options { scan | avmonitor | quarantine } Enable/disable POP3 AntiVirus scanning, monitoring, and quarantine.
    scan Enable POP3 antivirus scanning.
    avmonitor Enable POP3 antivirus logging.
    quarantine Enable POP3 antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested Block nested archives.
    mailbomb Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested Log nested archives.
    mailbomb Log mail bomb archives.
    unhandled Log archives that FortiOS cannot open.
set emulator { enable | disable } Enable/disable the virus emulator.
set executables { default | virus } Treat Windows executable files as viruses for the purpose of blocking or monitoring.
    default Perform standard AntiVirus scanning of Windows executable files.
    virus Treat Windows executables as viruses.
set options { scan | avmonitor | quarantine } Enable/disable SMTP AntiVirus scanning, monitoring, and quarantine.
    scan Enable SMTP antivirus scanning.
    avmonitor Enable SMTP antivirus logging.
    quarantine Enable SMTP antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested Block nested archives.
    mailbomb Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested Log nested archives.
    mailbomb Log mail bomb archives.
```

```
        unhandled Log archives that FortiOS cannot open.
set emulator { enable | disable } Enable/disable the virus emulator.
set executables { default | virus } Treat Windows executable files as viruses for the purpose of blocking or monitoring.
    default Perform standard AntiVirus scanning of Windows executable files.
    virus Treat Windows executables as viruses.
set options { scan | avmonitor | quarantine } Enable/disable MAPI AntiVirus scanning, monitoring, and quarantine.
    scan Enable MAPI antivirus scanning.
    avmonitor Enable MAPI antivirus logging.
    quarantine Enable MAPI antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested Block nested archives.
    mailbomb Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested Log nested archives.
    mailbomb Log mail bomb archives.
    unhandled Log archives that FortiOS cannot open.
set emulator { enable | disable } Enable/disable the virus emulator.
set executables { default | virus } Treat Windows executable files as viruses for the purpose of blocking or monitoring.
    default Perform standard AntiVirus scanning of Windows executable files.
    virus Treat Windows executables as viruses.
set options { scan | avmonitor | quarantine } Enable/disable NNTP AntiVirus scanning, monitoring, and quarantine.
    scan Enable NNTP antivirus scanning.
    avmonitor Enable NNTP antivirus logging.
    quarantine Enable NNTP antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option } Select the archive types to block.
    encrypted Block encrypted archives.
    corrupted Block corrupted archives.
    multipart Block multipart archives.
    nested Block nested archives.
    mailbomb Block mail bomb archives.
    unhandled Block archives that FortiOS cannot open.
set archive-log { option } Select the archive types to log.
    encrypted Log encrypted archives.
    corrupted Log corrupted archives.
    multipart Log multipart archives.
    nested Log nested archives.
```

```
        mailbomb    Log mail bomb archives.
        unhandled  Log archives that FortiOS cannot open.
set emulator { enable | disable }  Enable/disable the virus emulator.
set options { scan | avmonitor | quarantine }  Enable/disable SMB AntiVirus scanning, monitoring, and quarantine.
        scan        Enable SMB antivirus scanning.
        avmonitor   Enable SMB antivirus logging.
        quarantine  Enable SMB antivirus quarantine. Files are quarantined depending on quarantine settings.
set archive-block { option }  Select the archive types to block.
        encrypted  Block encrypted archives.
        corrupted  Block corrupted archives.
        multipart  Block multipart archives.
        nested     Block nested archives.
        mailbomb   Block mail bomb archives.
        unhandled  Block archives that FortiOS cannot open.
set archive-log { option }  Select the archive types to log.
        encrypted  Log encrypted archives.
        corrupted  Log corrupted archives.
        multipart  Log multipart archives.
        nested     Log nested archives.
        mailbomb   Log mail bomb archives.
        unhandled  Log archives that FortiOS cannot open.
set emulator { enable | disable }  Enable/disable the virus emulator.
set infected { none | quar-src-ip }  Enable/Disable quarantining infected hosts to the banned user list.
        none       Do not quarantine infected hosts.
        quar-src-ip Quarantine all traffic from the infected hosts source IP.
set expiry { string }  Duration of quarantine.
set log { enable | disable }  Enable/disable AntiVirus quarantine logging.
set av-virus-log { enable | disable }  Enable/disable AntiVirus logging.
set av-block-log { enable | disable }  Enable/disable logging for AntiVirus file blocking.
set scan-mode { quick | full }  Choose between full scan mode and quick scan mode.
        quick      Use quick mode scanning. Quick mode uses a smaller database and may be less accurate. Full mode is recommended.
        full       Full mode virus scanning. Recommended scanning mode. More accurate than quick mode with similar performance.
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

comment <string>

Add a comment to the profile.

replacemsg-group <group-name>

Set a replacement message group to use with antivirus scanning.

inspection-mode {proxy | flow-based}

Set the inspection mode. Select between the following options:

- `proxy`: Scanning reconstructs content passing through the FortiGate unit and inspects the content for security threats.
- `flow-based`: Scanning takes a snapshot of content packets and uses pattern matching to identify security threats in the content.

The default is `proxy`. For more information, see [Inspection Modes](#).

ftgd-analytics {disable}

Choose which files are sent to FortiSandbox for further inspection. Select between the following options:

- `disable`: No files are sent for inspection.
- `suspicious`: Files that the antivirus engine deems suspicious as sent for inspection.
- `everything`: All files are sent for inspection.

The default is `disable`.

analytics-db {enable | disable}

Enable or disable using antivirus signatures from the FortiSandbox's database as well as signatures from the FortiGate. Disabled by default.

mobile-malware-db {enable | disable}

Enable or disable using antivirus signatures from the mobile malware signature database as well as signatures from the FortiGate. Enabled by default.

config {http | ftp | imap | pop3 | smtp | smb}

Configure how this profile handles specific protocols.

options {scan | avmonitor | quarantine}

Set an action to apply to traffic using this protocol. Select from the following options:

- `scan`: Scan files transferred using this protocol for viruses.
- `avmonitor`: Log detected viruses, but allow them through the firewall without modification.
- `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGates with a hard disk or those connected to a FortiAnalyzer.

archive-block {encrypted | corrupted | multipart | nested | mailbomb | unhandled}

Set which types of archived files to block.

archive-log {encrypted | corrupted | multipart | nested | mailbomb | unhandled}

Set which types of archived files to log.

emulator {enable | disable}

Enable or disable the virus emulator. Enabled by default.

executables {default | virus}

Set how this profile treats executable files sent with this protocol. Select from the following options:

- `default`: Perform standard antivirus scanning.
- `virus`: Treat executable files as viruses.

The default option is `default`. This option is only available for IMAP, POP3, and SMTP.

config nac-quar

Configure the quarantine settings for this profile.

infected {none | quar-src-ip}

Set which infected hosts are added to the banned user list. Select from the following options:

- `none`: No hosts are banned.
- `quar-src-ip`: All traffic from the source IP is banned.

The default is `none`.

expiry <duration>

Set the duration of the quarantine in the days, hours, minutes format `<###d##h##m>`. The default is 5 minutes. This option only appears if `infected` is set to `quar-src-ip`.

log {enable | disable}

Enable or disable logging for antivirus quarantines. Disabled by default.

av-virus-log {enable | disable}

Enable or disable logging for antivirus scanning. Enabled by default.

av-block-log {enable | disable}

Enable or disable logging files that are blocked by antivirus. Enabled by default.

scan-mode {quick | full}

Choose which scan mode to use for antivirus inspection. Select from the following options:

- `quick`: This mode uses a compact antivirus database and advanced techniques to improve performance.
- `full`: In this mode, content packets are buffered while simultaneously being sent to their destination.

The default is `full`. These options are only available when `inspection-mode` is set to `flow-based`.

antivirus quarantine

Configure the antivirus quarantine options. **Note:** MM1, MM3, MM4, and MM7 traffic types supported only in FortiOS Carrier.

```
config antivirus quarantine
  set agelimit { integer }   Age limit for quarantined files (0 - 479 hours, 0 means forever). range[0-479]
  set maxfilesize { integer } Maximum file size to quarantine (0 - 500 Mbytes, 0 means unlimited). range[0-500]
  set quarantine-quota { integer } The amount of disk space to reserve for quarantining files (0 - 4294967295 Mbytes, depends on disk space).
range[0-4294967295]
  set drop-infected { option } Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead
of being quarantined.
    imap  IMAP.
    smtp  SMTP.
    pop3  POP3.
    http  HTTP.
    ftp   FTP.
    nntp  NNTP.
    imaps IMAPS.
    smtps SMTPS.
    pop3s POP3S.
    https HTTPS.
    ftps  FTPS.
    mapi  MAPI.
    cifs  CIFS.
  set store-infected { option } Quarantine infected files found in sessions using the selected protocols.
    imap  IMAP.
    smtp  SMTP.
    pop3  POP3.
    http  HTTP.
    ftp   FTP.
    nntp  NNTP.
    imaps IMAPS.
    smtps SMTPS.
    pop3s POP3S.
    https HTTPS.
    ftps  FTPS.
    mapi  MAPI.
    cifs  CIFS.
  set drop-blocked { option } Do not quarantine dropped files found in sessions using the selected protocols. Dropped files are deleted instead
```

of being quarantined.

```
imap    IMAP.  
smtp    SMTP.  
pop3    POP3.  
http    HTTP.  
ftp     FTP.  
nntp    NNTP.  
imaps   IMAPS.  
smtps   SMTPS.  
pop3s   POP3S.  
ftps    FTPS.  
mapi    MAPI.  
cifs    CIFS.
```

```
set store-blocked { option }   Quarantine blocked files found in sessions using the selected protocols.
```

```
imap    IMAP.  
smtp    SMTP.  
pop3    POP3.  
http    HTTP.  
ftp     FTP.  
nntp    NNTP.  
imaps   IMAPS.  
smtps   SMTPS.  
pop3s   POP3S.  
ftps    FTPS.  
mapi    MAPI.  
cifs    CIFS.
```

```
set drop-heuristic { option }   Do not quarantine files detected by heuristics found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.
```

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

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

```
imap    IMAP.
```

```
smtp    SMTP.
pop3    POP3.
http    HTTP.
ftp     FTP.
nntp    NNTP.
imaps   IMAPS.
smtps   SMTPS.
pop3s   POP3S.
https   HTTPS.
ftps    FTPS.
mapi    MAPI.
cifs    CIFS.

set lowspace { drop-new | ovrw-old }  Select the method for handling additional files when running low on disk space.
drop-new Drop (delete) the most recently quarantined files.
ovrw-old Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.

set destination { NULL | disk | FortiAnalyzer }  Choose whether to quarantine files to the FortiGate disk or to FortiAnalyzer or to delete them
instead of quarantining them.
NULL      Files that would be quarantined are deleted.
disk      Quarantine files to the FortiGate hard disk.
FortiAnalyzer FortiAnalyzer

end
```

Supplemental Information

The following section is for those commands that require further explanation.

agelimit <int>

Set the age limit for how long files are kept in quarantine. 0 means files are kept forever. The default is 0. This option appears when `destination` is not set to `NULL`.

maxfilesize <int>

Specify, in MB, the maximum file size to quarantine. 0 means unlimited. The default is 0.

quarantine-quota <int>

Set the antivirus quarantine quota in MB, which is the amount of disk space to reserve for quarantining files. 0 means unlimited. The default is 0.

drop-infected {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}

Drop infected files found in traffic for the specified protocols. By default, no files are dropped.

store-infected {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}

Quarantine virus infected files found in traffic for the specified protocols. By default, all protocols are specified.

drop-blocked {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}

Drop blocked files found in traffic for the specified protocols. By default, no files are dropped.

store-blocked {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}

Quarantine blocked files found in traffic for the specified protocols. By default, all protocols are specified.

drop-heuristic {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}

Drop files found by heuristic scanning in traffic for the specified protocols. By default, no files are dropped.

store-heuristic {imap | smtp | pop3 | http | ftp | nntp | imaps | smtps | pop3s | https | ftps | mapi | mm1 | mm3 | mm4 | mm7}

Quarantine files found by heuristic scanning in traffic for the specified protocols. By default, all protocols are specified.

drop-intercepted {imap | smtp | pop3 | http | ftp | mm1 | mm3 | mm4 | mm7}

For FortiOS Carrier, drop intercepted files found in traffic for the specified protocols. By default, no files are dropped.

store-intercepted {imap | smtp | pop3 | http | ftp | mm1 | mm3 | mm4 | mm7}

For FortiOS Carrier, quarantine intercepted files found in traffic for the specified protocols. By default, all protocols are specified.

lowspace {drop-new | ovrw-old}

Select the method for handling additional quarantined files when the FortiGate hard disk is running out of space. Select from the following options:

- `drop-new`: Drop new quarantine files.
- `ovrw-old`: Overwrite the oldest file (lowest TTL).

The default is `ovrw-old`.

destination {NULL | disk | FortiAnalyzer}

Set the destination where files are quarantined. Select from the following options:

- `NULL`: No files are quarantined.
- `disk`: Files are quarantined using the FortiGate's hard disk (if present).
- `FortiAnalyzer`: Files are quarantined using a FortiAnalyzer.

If the FortiGate has a hard disk, the default is `disk`. If no hard disk is available, the default is `NULL`.

antivirus settings

Configure basic antivirus settings.

```
config antivirus settings
  set default-db { normal | extended | extreme }  Select the AV database to be used for AV scanning.
    normal    Use the normal AntiVirus database.
    extended  Use the extended AntiVirus database.
    extreme   Use all available AntiVirus databases
  set grayware { enable | disable }  Enable/disable grayware detection when an AntiVirus profile is applied to traffic.
end
```

Supplemental Information

The following section is for those commands that require further explanation.

default-db {normal | extended | extreme}

Select the database to be used for antivirus scanning. Both proxy and flow inspection modes use these databases.

- **normal**: use the normal virus database, which includes viruses that are "in the wild," including the commonly seen viruses. For regular antivirus protection, it is sufficient to use this database.
- **extended**: use the extended virus database, which includes both "in the wild" viruses and a large collection of "in the zoo" viruses. It is suitable for an enhanced security environment.
- **extreme**: use the extreme virus database, which includes both "in the wild" viruses and all available "in the zoo" viruses. It is suitable for an enhanced security environment.

The default is `normal`.

grayware {enable | disable}

Enable or disable the detection of grayware, including adware, dial, downloader, hacker tool, keylogger, RAT, and spyware. The is enabled by default.

application

Use these commands to configure application control.

This section includes syntax for the following commands:

- [application custom](#)
- [application list](#)
- [application name](#)
- [application rule-settings](#)

application custom

Configure a custom firewall application.

```
config application custom
  edit { tag }
  # Configure custom application signatures.
  set tag { string } Signature tag. size[63]
  set name { string } Name of this custom application signature. size[63]
  set id { integer } Custom application category ID (use ? to view available options). range[0-4294967295]
  set comment { string } Comment. size[63]
  set signature { string } The text that makes up the actual custom application signature. size[1023]
  set category { integer } Custom application category ID (use ? to view available options). range[0-4294967295]
  set protocol { string } Custom application signature protocol.
  set technology { string } Custom application signature technology.
  set behavior { string } Custom application signature behavior.
  set vendor { string } Custom application signature vendor.
  next
end
```

The following options are not configurable:

- id
- name

comment <string>

Add a comment to the custom application.

signature <string>

Set the application signature. For information about custom application signatures, see [Custom Application & IPS Signatures](#).

category <ID>

Set the category ID. Type `set category ?` to view all available options.

protocol <ID>

Set the protocol ID. Type `set protocol ?` to view all available options.

technology <ID>

Set the technology ID. Type `set technology ?` to view all available options.

vendor <ID>

Set the vendor ID. Type `set vendor ?` to view all available options.

application list

Configure an application control list.

```
config application list
  edit { name }
  # Configure application control lists.
  set name { string } List name. size[35]
  set comment { string } comments size[255]
  set replacemsg-group { string } Replacement message group. size[35] - datasource(s): system.replacemsg-group.name
  set other-application-action { pass | block } Action for other applications.
    pass Allow sessions matching an application in this application list.
    block Block sessions matching an application in this application list.
  set app-replacemsg { disable | enable } Enable/disable replacement messages for blocked applications.
  set other-application-log { disable | enable } Enable/disable logging for other applications.
  set unknown-application-action { pass | block } Pass or block traffic from unknown applications.
    pass Pass or allow unknown applications.
    block Drop or block unknown applications.
  set unknown-application-log { disable | enable } Enable/disable logging for unknown applications.
  set p2p-black-list { skype | edonkey | bittorrent } P2P applications to be black listed.
    skype Skype.
    edonkey Edonkey.
    bittorrent Bit torrent.
  set deep-app-inspection { disable | enable } Enable/disable deep application inspection.
  set options { option } Basic application protocol signatures allowed by default.
    allow-dns Allow DNS.
    allow-icmp Allow ICMP.
    allow-http Allow generic HTTP web browsing.
    allow-ssl Allow generic SSL communication.
    allow-quic Allow QUIC.
  config entries
    edit { id }
    # Application list entries.
    set id { integer } Entry ID. range[0-4294967295]
    config risk
      edit { level }
      # Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).
      set level { integer } Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). range[0-4294967295]
```

```
    next
config category
  edit { id }
  # Category ID list.
  set id { integer } Application category ID. range[0-4294967295]
  next
config sub-category
  edit { id }
  # Application Sub-category ID list.
  set id { integer } Application sub-category ID. range[0-4294967295]
  next
config application
  edit { id }
  # ID of allowed applications.
  set id { integer } Application IDs. range[0-4294967295]
  next
set protocols { string } Application protocol filter.
set vendor { string } Application vendor filter.
set technology { string } Application technology filter.
set behavior { string } Application behavior filter.
set popularity { option } Application popularity filter (1 - 5, from least to most popular).
  1 Popularity level 1.
  2 Popularity level 2.
  3 Popularity level 3.
  4 Popularity level 4.
  5 Popularity level 5.
config tags
  edit { name }
  # Tag filter.
  set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
config parameters
  edit { id }
  # Application parameters.
  set id { integer } Parameter ID. range[0-4294967295]
  set value { string } Parameter value. size[63]
  next
set action { pass | block | reset } Pass or block traffic, or reset connection for traffic from this application.
  pass Pass or allow matching traffic.
  block Block or drop matching traffic.
  reset Reset sessions for matching traffic.
set log { disable | enable } Enable/disable logging for this application list.
set log-packet { disable | enable } Enable/disable packet logging.
```

```

set rate-count { integer } Count of the rate. range[0-65535]
set rate-duration { integer } Duration (sec) of the rate. range[1-65535]
set rate-mode { periodical | continuous } Rate limit mode.
    periodical Allow configured number of packets every rate-duration.
    continuous Block packets once the rate is reached.
set rate-track { option } Track the packet protocol field.
    none none
    src-ip Source IP.
    dest-ip Destination IP.
    dhcp-client-mac DHCP client.
    dns-domain DNS domain.
set session-ttl { integer } Session TTL (0 = default). range[0-4294967295]
set shaper { string } Traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set shaper-reverse { string } Reverse traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set per-ip-shaper { string } Per-IP traffic shaper. size[35] - datasource(s): firewall.shaper.per-ip-shaper.name
set quarantine { none | attacker } Quarantine method.
    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.
    set quarantine-expiry { string } Duration of quarantine, from 1 minute to 364 days, 23 hours, and 59 minutes from now. (format:
###d##h##m, default = 5m). Requires quarantine set to attacker.
    set quarantine-log { disable | enable } Enable/disable quarantine logging.
next
end

```

comment <string>

Add a comment to the control list.

replacemsg-group <group-name>

Select a replacement message group to use for the control list.

other-application-action {pass | block}

Set the action to take for traffic from other applications. The default is `pass`.

app-replacemsg {enable | disable}

Enable or disable replacement messages for blocked application traffic. Default is `enable`.

other-application-log {enable | disable}

Enable or disable logging traffic from other applications. Default is `disable`.

unknown-application-action {pass | block}

Set an action to take for traffic from unknown applications. The default is `pass`.

unknown-application-log {enable | disable}

Enable or disable logging traffic from unknown applications. Default is `disable`.

p2p-black-list {skype | edonkey | bittorrent}

Add P2P applications to a blacklist.

options {allow-dns | allow-icmp | allow-http | allow-ssl}

Set which basic application protocols are allowed by default. Select from the following options:

- `allow-dns`: Allow DNS traffic
- `allow-icmp`: Allow ICMP traffic
- `allow-http`: Allow generic HTTP web browsing
- `allow-ssl`: Allow generic SSL communication

The default is `allow-dns`.

config entries

Configure entries on the application control list.

risk <level>

Set the risk level for the applications. Select from the following options:

- 1: Low
- 2: Elevated
- 3: Medium
- 4: High
- 5: Critical

category <ID>

Set the application category. Type `set category ?` to view all options.

sub-category <ID>

Set the application sub-category. Type `set sub-category ?` to view all options. Enter `all` to include all sub-categories.

application <ID>

Set which applications are allowed. Type `set application ?` to view all options.

protocols <ID>

Set which protocols are allowed. Type `set protocols ?` to view all options. The default is `all`.

vendor <ID>

Set which application vendors are allowed. Type `set vendor ?` to view all options. The default is `all`.

technology {all | 0 | 1 | 2 | 4}

Select the technologies involved in these applications. Select from the following options:

- `all`: All technologies
- `0`: Network-Protocol
- `1`: Browser-Based
- `2`: Client-Server
- `4`: Peer-to-Peer

The default is `all`.

behavior {all | 2 | 3 | 5 | 6 | 9}

Select the application behaviors filter. Select from the following options:

- `all`: Apply all behaviors
- `2`: Botnet
- `3`: Evasion
- `5`: Excessive bandwidth
- `6`: Tunneling
- `9`: Cloud

The default is `all`.

popularity {1 | 2 | 3 | 4 | 5}

Enter the popularity levels of this application, with 1 being the least popular and 5 being the most popular. The default is `1 2 3 4 5`.

tags <string>

Assign object tags.

action {pass | block | reset}

Select the action to apply to matching traffic from the following options:

- `pass`: Allow traffic from the specified application(s)
- `block`: Stop traffic from the specified application(s)
- `reset`: Reset the network connection

The default is `block`.

log {enable | disable}

Enable or disable logging for traffic from this list entry. The default is `enable`.

log-packet {enable | disable}

Enable or disable packet logging for traffic from this list entry. The default is `disable`.

session-ttl <int>

Set the Session TTL. The default is `0`.

quarantine {none | attacker}

Set quarantine options for when an attack is detected. The default is `none`.

application name

Use this command to view the application category and ID of each application. This command is read only and cannot be used to change application settings.

```
config application name
  edit { name }
  # Configure application signatures.
  set name { string } Application name. size[63]
  set id { integer } Application ID. range[0-4294967295]
  set category { integer } Application category ID. range[0-4294967295]
  set sub-category { integer } Application sub-category ID. range[0-255]
  set popularity { integer } Application popularity. range[0-255]
  set risk { integer } Application risk. range[0-255]
  set weight { integer } Application weight. range[0-255]
  set protocol { string } Application protocol.
  set technology { string } Application technology.
  set behavior { string } Application behavior.
  set vendor { string } Application vendor.
  set parameter { string } Application parameter name. size[35]
config metadata
  edit { id }
  # Meta data.
  set id { integer } ID. range[0-4294967295]
  set metaid { integer } Meta ID. range[0-4294967295]
  set valueid { integer } Value ID. range[0-4294967295]
next
end
```

config application name <application-name>

The name of the application to view. Enter the first letter(s) of the name then use the **Tab** button to get the correct name. You can also type ? to view all options.

get

Use get to view information about the application.

application rule-settings

Configure application rule settings.

```
config application rule-settings
  edit { id }
  # Configure application rule settings.
  set id { integer } Rule ID. range[0-4294967295]
  config tags
    edit { name }
    # Object tag of the application rule ID.
    set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
next
end
```

config application rule-settings <ID>

The ID for the rule settings entry.

tags <tag-name>

The tags for the rule settings entry.

authentication

Use these commands to configure application control.

This section includes syntax for the following commands:

- [authentication rule](#)
- [authentication scheme](#)
- [authentication setting](#)

authentication rule

Configure authentication rules.

```
config authentication rule
  edit { name }
  # Configure Authentication Rules.
  set name { string } Authentication rule name. size[35]
  set status { enable | disable } Enable/disable this authentication rule.
  set protocol { http | ftp | socks } Select the protocol to use for authentication (default = http). Users connect to the FortiGate using
this protocol and are asked to authenticate.
    http Use HTTP for authentication.
    ftp Use FTP for authentication.
    socks Use SOCKS for authentication.
  config srcaddr
    edit { name }
    # Select an IPv4 source address from available options. Required for web proxy authentication.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name,firewall.proxy-address.-
name,firewall.proxy-addrgrp.name
    next
  config srcaddr6
    edit { name }
    # Select an IPv6 source address. Required for web proxy authentication.
    set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
    next
  set ip-based { enable | disable } Enable/disable IP-based authentication. Once a user authenticates all traffic from the IP address the
user authenticated from is allowed.
  set active-auth-method { string } Select an active authentication method. size[35] - datasource(s): authentication.scheme.name
  set sso-auth-method { string } Select a single-sign on (SSO) authentication method. size[35] - datasource(s): authentication.scheme.name
  set web-auth-cookie { enable | disable } Enable/disable Web authentication cookies (default = disable).
  set transaction-based { enable | disable } Enable/disable transaction based authentication (default = disable).
  set comments { string } Comment. size[1023]
  next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

status {enable | disable}

Enable (be default) or disable authentication rule status.

protocol {https | ftp | socks}

Matching protocol for authentication (default = http).

srcaddr

Source address or address group name, available for web proxy only. This command must be set.

srcaddr6

Source IPv6 address or address group name, available for web proxy only. This command must be set.

ip-based {enable | disable}

Enable (be default) or disable IP-based authentication.

active-auth-method <name>

Set the active authentication method using the scheme name.

sso-auth-method <name>

Set the Single-Sign-On authentication method using the scheme name.

web-auth-cookie {enable | disable}

Enable or disable (by default) the web authentication cookie.

transaction-based

Enable or disable (by default) transaction-based authentication.

comments

Configure an optional comment.

authentication scheme

Configure authentication schemes.

```
config authentication scheme
  edit { name }
  # Configure Authentication Schemes.
  set name { string } Authentication scheme name. size[35]
  set method { option } Authentication methods (default = basic).
    ntlm      NTLM authentication.
    basic     Basic HTTP authentication.
    digest    Digest HTTP authentication.
    form      Form-based HTTP authentication.
    negotiate Negotiate authentication.
    fssso     Fortinet Single Sign-On (FSSO) authentication.
    rssso     RADIUS Single Sign-On (RSSO) authentication.
  set negotiate-ntlm { enable | disable } Enable/disable negotiate authentication for NTLM (default = disable).
  set require-tfa { enable | disable } Enable/disable two-factor authentication (default = disable).
  set fssso-guest { enable | disable } Enable/disable user fssso-guest authentication (default = disable).
config user-database
  edit { name }
  # Authentication server to contain user information; "local" (default) or "123" (for LDAP).
  set name { string } Authentication server name. size[64] - datasource(s): system.datasource.name,user.radius.name,user.tacacs+.name,user.ldap.name,user.group.name
  next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

method {ntlm | basic | digest | form | negotiate | fssso | rssso}

Configure the authentication method for this scheme.

- **ntlm**: NTLM authentication.
- **basic**: Basic HTTP authentication (default).
- **digest**: Digest HTTP authentication.
- **form**: Form-based HTTP authentication.
- **negotiate**: Negotiate authentication.
- **fssso**: Fortinet Single Sign-On authentication.
- **rssso**: RADIUS Single Sign-On authentication.

negotiate-ntlm {enable | disable}

Enable or disable (by default) NTLM negotiation.

require-tfa {enable | disable}

Enable or disable (by default) two-factor authentication.

fssso-guest {enable | disable}

Enable or disable (by default) user fssso-guest.

user-database <source>

Configure the authentication server that contains user information; can be local, RADIUS, TACACS+, or LDAP.

authentication setting

Configure authentication settings.

```
config authentication setting
  set active-auth-scheme { string } Active authentication method (scheme name). size[35] - datasource(s): authentication.scheme.name
  set sso-auth-scheme { string } Single-Sign-On authentication method (scheme name). size[35] - datasource(s): authentication.scheme.name
  set captive-portal { string } Captive portal host name. size[255] - datasource(s): firewall.address.name
  set captive-portal-port { integer } Captive portal port number (1 - 65535, default = 0). range[1-65535]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

active-auth-scheme <name>

Set the active authentication method using the scheme name.

sso-auth-scheme <name>

Set the Single-Sign-On authentication method using the scheme name.

captive-portal <name>

Set the captive portal host name.

captive-portal-port [1 - 65535]

Set the captive portal port number, between 1 and 65535.

aws

Use this command to configure AWS settings.

This section includes syntax for the following command:

- [aws setting](#)

aws setting

Configure AWS settings.

```
config aws setting
  set access-key { string }  AWS access key. size[31]
  set secret-key { password_string }  AWS secret key. size[59]
  set region { string }  AWS region name. size[15]
  set vpc-id { string }  AWS VPC ID. size[15]
  set update-interval { integer }  AWS service update interval (60 - 600 sec, default = 60). range[60-600]
end
```

certificate

Use these commands to configure certificates.

This section includes syntax for the following commands:

- [certificate ca](#)
- [certificate crl](#)
- [certificate local](#)

certificate ca

Introduction.

```
config certificate ca
  edit { name }
  # CA certificate.
  set name { string } Name. size[79]
  set ca { string } CA certificate as a PEM file.
  set range { global | vdom } Either global or VDOM IP address range for the CA certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } CA certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  set trusted { enable | disable } Enable/disable as a trusted CA.
  set scep-url { string } URL of the SCEP server. size[255]
  set auto-update-days { integer } Number of days to wait before requesting an updated CA certificate (0 - 4294967295, 0 = disabled). range
[0-4294967295]
  set auto-update-days-warning { integer } Number of days before an expiry-warning message is generated (0 - 4294967295, 0 = disabled). range
[0-4294967295]
  set source-ip { ipv4 address } Source IP address for communications to the SCEP server.
  set last-updated { integer } Time at which CA was last updated. range[0-4294967295]
  next
end
```


certificate crl

Introduction.

```
config certificate crl
  edit { name }
  # Certificate Revocation List as a PEM file.
  set name { string } Name. size[35]
  set crl { string } Certificate Revocation List as a PEM file.
  set range { global | vdom } Either global or VDOM IP address range for the certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } Certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  set update-vdom { string } VDOM for CRL update. size[31] - datasource(s): system.vdom.name
  set ldap-server { string } LDAP server name for CRL auto-update. size[35]
  set ldap-username { string } LDAP server user name. size[63]
  set ldap-password { password_string } LDAP server user password. size[128]
  set http-url { string } HTTP server URL for CRL auto-update. size[255]
  set scep-url { string } SCEP server URL for CRL auto-update. size[255]
  set scep-cert { string } Local certificate for SCEP communication for CRL auto-update. size[35] - datasource(s): certificate.local.name
  set update-interval { integer } Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.
  range[0-4294967295]
  set source-ip { ipv4 address } Source IP address for communications to a HTTP or SCEP CA server.
  set last-updated { integer } Time at which CRL was last updated. range[0-4294967295]
  next
end
```

certificate local

Introduction.

```

config certificate local
  edit { name }
  # Local keys and certificates.
  set name { string } Name. size[35]
  set password { password_string } Password as a PEM file. size[128]
  set comments { string } Comment. size[511]
  set private-key { string } PEM format key, encrypted with a password.
  set certificate { string } PEM format certificate.
  set csr { string } Certificate Signing Request.
  set state { string } Certificate Signing Request State.
  set scep-url { string } SCEP server URL. size[255]
  set range { global | vdom } Either a global or VDOM IP address range for the certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } Certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  set auto-regenerate-days { integer } Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).
range[0-4294967295]
  set auto-regenerate-days-warning { integer } Number of days to wait before an expiry warning message is generated (0 = disabled). range[0-
4294967295]
  set scep-password { password_string } SCEP server challenge password for auto-regeneration. size[128]
  set ca-identifier { string } CA identifier of the CA server for signing via SCEP. size[255]
  set name-encoding { printable | utf8 } Name encoding method for auto-regeneration.
    printable Printable encoding (default).
    utf8 UTF-8 encoding.
  set source-ip { ipv4 address } Source IP address for communications to the SCEP server.
  set ike-localid { string } Local ID the FortiGate uses for authentication as a VPN client. size[63]
  set ike-localid-type { asn1dn | fqdn } IKE local ID type.
    asn1dn ASN.1 distinguished name.
    fqdn Fully qualified domain name.
  set last-updated { integer } Time at which certificate was last updated. range[0-4294967295]
next

```

end

dlp

Use these commands to configure Data Leak Prevention (DLP).

This section includes syntax for the following commands:

- [dlp filepattern](#)
- [dlp fp-doc-source](#)
- [dlp fp-sensitivity](#)
- [dlp sensor](#)
- [dlp settings](#)

dlp filepattern

Use this command to add, edit or delete the file patterns used for DLP file blocking and to set which protocols to check for files to block.

```
config dlp filepattern
  edit { id }
  # Configure file patterns used by DLP blocking.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table containing the file pattern list. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { pattern }
    # Configure file patterns used by DLP blocking.
    set filter-type { pattern | type } Filter by file name pattern or by file type.
      pattern Filter by file name pattern.
      type Filter by file type.
    set pattern { string } Add a file name pattern. size[79]
    set file-type { option } Select a file type.
      7z Match 7-zip files.
      arj Match arj compressed files.
      cab Match Windows cab files.
      lzh Match lzh compressed files.
      rar Match rar archives.
      tar Match tar files.
      zip Match zip files.
      bzip Match bzip files.
      gzip Match gzip files.
      bzip2 Match bzip2 files.
      xz Match xz files.
      bat Match Windows batch files.
      msc Match msc files.
      uue Match uue files.
      mime Match mime files.
      base64 Match base64 files.
      binhex Match binhex files.
      elf Match elf files.
      exe Match Windows executable files.
      hta Match hta files.
      html Match html files.
```

```
jad          Match jad files.
class       Match class files.
cod         Match cod files.
javascript  Match javascript files.
msoffice    Match MS-Office files. For example, doc, xls, ppt, and so on.
msofficex  Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.
fsg        Match fsg files.
upx        Match upx files.
petite     Match petite files.
aspack     Match aspack files.
prc        Match prc files.
sis        Match sis files.
hlp        Match Windows help files.
activemime Match activemime files.
jpeg       Match jpeg files.
gif        Match gif files.
tiff       Match tiff files.
png        Match png files.
bmp        Match bmp files.
ignored    Match ignored files.
unknown    Match unknown files.
mpeg       Match mpeg files.
mov        Match mov files.
mp3        Match mp3 files.
wma        Match wma files.
wav        Match wav files.
pdf        Match Acrobat pdf files.
avi        Match avi files.
rm         Match rm files.
torrent    Match torrent files.
hibun     Match hibun files.
msi        Match Windows Installer msi files.
```

```
next
```

```
next
```

```
end
```

Supplemental Information

The following section is for those commands that require further explanation.

edit <filepattern_list_int>

A unique integer to identify the file pattern list. `edit ?` displays existing file pattern lists and their names. Range: 0 - 4294967295.

name <string>

Name of table containing the file pattern list.

comment <string>

Enter optional comment. The comment appears in the DLP sensor list and can remind you of the details of the sensor.

config entries

Configure file patterns used by DLP blocking.

edit <filepattern_str>

The name of the file pattern being configured. This can be any character string.

filter-type {pattern | type}

Filter by file name pattern or by file type. Default is `pattern`.

- `pattern`: filter based on the file name. The pattern may include wildcards (*). For example, blocking `*.scr` will stop all files with an `.scr` file extension.
- `type`: filter based on examination of the file contents, regardless of the file name. If you block the file type Archive (zip), all zip archives are blocked even if named with a different file extension.

file-type <string>

This command is only available and valid when `filter-type` is set to `type`. `set file-type ?` displays all available options.

This file type filter will examine the file contents to determine the type of file and look for a match to the `file-type` specified. The file name and file extension are ignored. Because of the way the file type filter works, renaming files to make them appear to be of a different type will not allow them past the FortiGate unit without detection.

Two of the available options are not file types:

- `unknown`: to configure a rule affecting every file format the file type filter unit does not recognize. Unknown includes every file format not available in the `file-type` command.
- `ignored`: to configure a rule affecting traffic the FortiGate unit typically does not scan. This includes primarily streaming audio and video.

dlp fp-doc-source

Use this command to add fingerprinting document sources including the server and filepath for the source files.

```
config dlp fp-doc-source
edit { name }
# Create a DLP fingerprint database by allowing the FortiGate to access a file server containing files from which to create fingerprints.
set name { string } Name of the DLP fingerprint database. size[35]
set server-type { samba } Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.
    samba SAMBA server.
set server { string } IPv4 or IPv6 address of the server. size[35]
set period { none | daily | weekly | monthly } Frequency for which the FortiGate checks the server for new or changed files.
    none Check the server when the FortiGate starts up.
    daily Check the server once a day.
    weekly Check the server once a week.
    monthly Check the server once a month.
set vdom { mgmt | current } Select the VDOM that can communicate with the file server.
    mgmt Communicate with the file server through the management VDOM.
    current Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.
set scan-subdirectories { enable | disable } Enable/disable scanning subdirectories to find files to create fingerprints from.
set scan-on-creation { enable | disable } Enable to keep the fingerprint database up to date when a file is added or changed on the server.
set remove-deleted { enable | disable } Enable to keep the fingerprint database up to date when a file is deleted from the server.
set keep-modified { enable | disable } 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.
set username { string } User name required to log into the file server. size[35]
set password { password_string } Password required to log into the file server. size[128]
set file-path { string } Path on the server to the fingerprint files (max 119 characters). size[119]
set file-pattern { string } Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards. size[35]
set sensitivity { string } Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using fp-sens-
itivity. size[35] - datasource(s): dlp.fp-sensitivity.name
set tod-hour { integer } Hour of the day on which to scan the server (0 - 23, default = 1). range[0-23]
set tod-min { integer } Minute of the hour on which to scan the server (0 - 59). range[0-59]
set weekday { option } Day of the week on which to scan the server.
    sunday Sunday
    monday Monday
    tuesday Tuesday
    wednesday Wednesday
    thursday Thursday
    friday Friday
```

```
        saturday  Saturday
    set date { integer }  Day of the month on which to scan the server (1 - 31). range[1-31]
    next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

edit <name_string>

Identify the server to which DLP will be applied.

server-type {samba}

Enter the type of DLP server. Currently only Samba (SMB) servers are supported.

server <string>

The IPv4 or IPv6 address of the server.

period {none | daily | weekly | monthly}

Select the frequency for server checking. Default is `none`.

vdom {mgmt | current}

Choose whether to perform document fingerprinting from the current VDOM or the management VDOM. Files might be accessible through the management VDOM that are not accessible through the current VDOM. Default is `mgmt`.

scan-subdirectories {enable | disable}

Enable/disable scanning of subdirectories while fingerprinting documents. Default is `enable`.

scan-on-creation {enable | disable}

Enable/disable force scan of server when document source is created or edited. Only appears if the period is set to `daily`, `weekly`, or `monthly`. Default is `enable`.

remove-deleted {enable | disable}

Enable/disable removing chunks of files deleted from the server. Default is `enable`.

keep-modified {enable | disable}

Enable/disable retaining old chunks of modified files. Default is `enable`.

username <string>

Samba server login username.

password <password>

Samba server login password.

file-path <string>

Path to file on the server.

file-pattern <string>

The file pattern to match when using DLP blocking. Can include wildcards and should include file type. For example, you would enter `set file-pattern "*fortinet.xls"` to match all files that end in `fortinet.xls`.

sensitivity <string>

Sensitivity labels must be created with `config dlp fp-sensitivity` before using this command. Specify a sensitivity label to apply to source files. `set sensitivity ?` displays all available labels.

tod-hour <integer>

Time of day to run scans. Enter the hour only and use 24-hour clock. Only appears if the period is set to `daily`, `weekly`, or `monthly`. Default is `1`.

tod-min <integer>

Time of day to run scans. Enter the minute only. This will only appear if the period is set to `daily`, `weekly`, or `monthly`. Default is `0`.

weekday {sunday | monday | tuesday | wednesday | thursday | friday | saturday}

Day of the week to run scans. This will only appear if the period is set to `weekly`. Default is `sunday`.

date <integer>

Date of the month to run scans. This will only appear if the period is set to `monthly`. Range: 1 - 31. Default is 1.

dlp fp-sensitivity

Use this command to add fingerprinting sensitivity labels that can be applied to document sources and DLP rules

```
config dlp fp-sensitivity
  edit { name }
  # Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source.
  set name { string } DLP Sensitivity Levels. size[35]
  next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

edit <name_string>

Enter a self-explanatory string for DLP sensitivity level. It will be used when setting `sensitivity` under `config fp-doc-source`. Entering `edit ?` displays all existing sensitivity levels.

dlp sensor

Use this command to create a DLP sensor. The DLP sensor includes settings such as action, archive, and severity for each rule or compound rule. A number of preconfigured sensors are provided with your FortiGate. These can be edited to more closely match your needs. Consult the Handbook's discussion of [data leak prevention concepts](#) for more detail.

```
config dlp sensor
  edit { name }
  # Configure DLP sensors.
  set name { string } Name of the DLP sensor. size[35]
  set comment { string } Comment. size[255]
  set replacemsg-group { string } Replacement message group used by this DLP sensor. size[35] - datasource(s): system.replacemsg-group.name
  config filter
    edit { id }
    # Set up DLP filters for this sensor.
    set id { integer } ID. range[0-4294967295]
    set name { string } Filter name. size[35]
    set severity { option } Select the severity or threat level that matches this filter.
      info      Informational.
      low       Low.
      medium    Medium.
      high      High.
      critical  Critical.
    set type { file | message } Select whether to check the content of messages (an email message) or files (downloaded files or email
  attachments).
      file      Check the contents of downloaded or attached files.
      message   Check the contents of email messages, web pages, etc.
    set proto { option } Check messages or files over one or more of these protocols.
      smtp      SMTP.
      pop3      POP3.
      imap      IMAP.
      http-get  HTTP GET.
      http-post HTTP POST.
      ftp       FTP.
      nntp      NNTP.
      mapi      MAPI
    set filter-by { option } Select the type of content to match.
      credit-card Match credit cards.
```

```

        ssn          Match social security numbers.
        regexp       Use a regular expression to match content.
        file-type    Match a DLP file pattern list.
        file-size    Match any file over with a size over the threshold.
        fingerprint  Match against a fingerprint sensitivity.
        watermark    Look for defined file watermarks.
        encrypted    Look for encrypted files.
    set file-size { integer } Match files this size or larger (0 - 4294967295 kbytes). range[0-4294967295]
    set company-identifier { string } Enter a company identifier watermark to match. Only watermarks that your company has placed on
the files are matched. size[35]
    config fp-sensitivity
        edit { name }
            # Select a DLP file pattern sensitivity to match.
            set name { string } Select a DLP sensitivity. size[35] - datasource(s): dlp.fp-sensitivity.name
        next
    set match-percentage { integer } Percentage of fingerprints in the fingerprint databases designated with the selected fp-sens-
itivity to match. range[0-100]
    set file-type { integer } Select the number of a DLP file pattern table to match. range[0-4294967295] - datasource(s): dlp.-
filepattern.id
    set regexp { string } Enter a regular expression to match (max. 255 characters). size[255]
    set archive { disable | enable } Enable/disable DLP archiving.
    set action { allow | log-only | block | quarantine-ip } Action to take with content that this DLP sensor matches.
        allow          Allow the content to pass through the FortiGate and do not create a log message.
        log-only       Allow the content to pass through the FortiGate, but write a log message.
        block          Block the content and write a log message.
        quarantine-ip  Quarantine all traffic from the IP address and write a log message.
    set expiry { string } Quarantine duration in days, hours, minutes format (dddhmm).
    next
set dlp-log { enable | disable } Enable/disable DLP logging.
set nac-quar-log { enable | disable } Enable/disable NAC quarantine logging.
set flow-based { enable | disable } Enable/disable flow-based DLP.
set full-archive-proto { option } Protocols to always content archive.
    smtp      SMTP.
    pop3      POP3.
    imap      IMAP.
    http-get  HTTP GET.
    http-post HTTP POST.
    ftp       FTP.
    nntp      NNTP.
    mapi      MAPI
set summary-proto { option } Protocols to always log summary.
    smtp      SMTP.
    pop3      POP3.

```

```
imap      IMAP.
http-get  HTTP GET.
http-post HTTP POST.
ftp       FTP.
nntp      NNTP.
mapi      MAPI
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

comment <string>

Enter an optional description of the DLP sensor. Descriptions with spaces must be enclosed in quotes.

replacemsg-group <group_name>

Specify which replacement message group to use.

dlp-log {enable | disable}

Enable/disable logging for data leak prevention. Default is `enable`.

nac-quar-log {enable | disable}

Enable or disable logging for network access control (NAC) quarantine creation. Default is `disable`.

flow-based {enable | disable}

Enable or disable flow-based DLP. Default is `disable`.

full-archive-proto {smtp | pop3 | imap | http-get | http-post ftp | nntp | mapi}

Enter the protocols to always content archive.

summary-proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}

Enter the protocols to always log summary.

config filter

Configure DLP filters.

edit <id_integer>

Specify ID of filter to be configured. Range: 0-4294967295. `edit ?` displays all existing filter IDs.

severity {info | low | medium | high | critical}

Set the event severity. Default is `medium`.

type {file | message}

Select whether to check messages (for example the content of an email message) or files (for example downloaded files or the content of files attached to an email). Default is `message`.

proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}

Identify the protocols to detect.

filter-by {credit-card | ssn | regexp | file-type | file-size | fingerprint | watermark | encrypted}

Select a filter for the sensor. Default is `credit-card`.

- `credit-card`: preconfigured sensor that logs the traffic, both files and messages, that contain credit card numbers in the formats used by American Express, MasterCard and Visa.
- `ssn`: preconfigured sensor that logs the traffic containing Social Security numbers with the exception of WebEx invitation emails.
- `watermark`: Match defined file watermarks. Fortinet provides a Linux-based utility that applies a digital watermark to files. The utility adds a small (approx. 100 byte) pattern to the file that is recognized by the DLP watermark filter. The pattern is invisible to the end user. Consult the Handbook's discussion of [data leak prevention concepts](#) for more detail.
- `encrypted`: Look for encrypted files. The filter is a binary one. If the files going through the policy is encrypted, the action is triggered.

regex <string>

The FortiGate checks network traffic for the regular expression specified in this regular expression filter. The regular expression library used by Fortinet is a variation of a library called PCRE (Perl Compatible Regular Expressions). Option appears when `type` is set to `file` and `filter-by` is set to `regex`.

file-type <integer>

File pattern table. Option appears when `type` is set to `file` and `filter-by` is set to `file-type`. Range: 0 - 4294967295.

file-size <integer>

Set the file size in KB. Files over this size will match with the filter. Option appears when `type` is set to `file` and `filter-by` is set to `file-size`. Range: 0-4294967295. Default is 0.

fp-sensitivity

Match against a fingerprint sensitivity. Option appears when `type` is set to `file` and `filter-by` is set to `fingerprint` or `watermark`. Fingerprinting must be configured in the CLI. See also [fp-doc-source](#) and [fp-sensitivity](#). Consult the Handbook's discussion of [data leak prevention concepts](#) for more detail.

match-percentage <integer>

Percentage of chunks required to constitute a match. Option appears when `type` is set to `file` and `filter-by` is set to `fingerprint`. Range: 0-100. Default is 0.

company-identifier

Company identifier for watermarking. Option appears when `type` is set to `file` and `filter-by` is set to `watermark`. Ensures that you are only blocking watermarks that your company has placed on the files, not watermarks with the same name but place by other companies.

action {allow | log-only | block | quarantine-ip}

Specify action to take when a match is detected. Default is `allow`.

- `allow`: no action is taken even if the patterns specified in the filter are matched.
- `log-only`: the FortiGate will take no action on network traffic matching a rule with this action. The filter match is logged
- `block`: traffic matching a filter with the block action will not be delivered.
- `quarantine-ip`: block access through the FortiGate unit for any IP address that sends traffic matching a sensor with this action. The IP address is added to the Banned User list for a duration of time that is determined by `set expiry`.

expiry <###d##h##m>

Set the duration of the quarantine in the days, hours, minutes format dddhmm ###d##h##m. Only appears if `action is set to quarantine-ip`. Range: 0d0h1m -364d23h59m. Default is 5m.

dlp settings

Use this command to designate logical storage settings for the DLP fingerprinting database.

```
config dlp settings
  set storage-device { string } Storage device name. size[35] - datasource(s): system.storage.name
  set size { integer } Maximum total size of files within the storage (MB). range[16-4294967295]
  set db-mode { stop-adding | remove-modified-then-oldest | remove-oldest } Behaviour when the maximum size is reached.
    stop-adding Stop adding entries.
    remove-modified-then-oldest Remove modified chunks first, then oldest file entries.
    remove-oldest Remove the oldest files first.
  set cache-mem-percent { integer } Maximum percentage of available memory allocated to caching (1 - 15%). range[1-15]
  set chunk-size { integer } Maximum fingerprint chunk size. **Changing will flush the entire database**. range[100-100000]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

storage device <string>

Enter the storage device name.

size <integer>

Enter the maximum total size of files in storage in MB. Default is 16.

db-mode {remove-modified-then-oldest | remove-oldest | stop-adding}

Select the method of maintaining the database size. Default is `stop-adding`.

- `remove-modified-then-oldest`: remove oldest chunks first, and then remove oldest file entries.
- `remove-oldest`: just remove the oldest files first.
- `stop-adding`: don't remove files, just stop adding to database.

cache-mem-percent <integer>

Enter the maximum percentage of available memory allocated to caching. Range: 1 - 15 %. Default is 2.

chunk-size <integer>

Maximum fingerprint chunk size.

Changing the chunk size will flush the entire database. Document source fingerprints will repopulate with the next scan. Only manually updated fingerprints will be lost. Range: 100 - 100000. Default is 2800. Smaller chunks allow for greater precision, but at the cost of increased processing, database size, and lookups.

dnsfilter

Use dnsfilter commands to configure domain filter lists and DNS filter profiles.

This section includes syntax for the following commands:

- [dnsfilter domain-filter](#)
- [dnsfilter profile](#)

dnsfilter domain-filter

Use this command to configure domain filter lists.

```
config dnsfilter domain-filter
  edit { id }
  # Configure DNS domain filters.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { id }
    # DNS domain filter entries.
    set id { integer } Id. range[0-4294967295]
    set domain { string } Domain entries to be filtered. size[511]
    set type { simple | regex | wildcard } DNS domain filter type.
      simple Simple domain string.
      regex Regular expression domain string.
      wildcard Wildcard domain string.
    set action { block | allow | monitor } Action to take for domain filter matches.
      block Block DNS requests matching the domain filter.
      allow Allow DNS requests matching the domain filter without logging.
      monitor Allow DNS requests matching the domain filter with logging.
    set status { enable | disable } Enable/disable this domain filter.
  next
end
```

dnsfilter profile

Use this command to configure DNS filter profiles.

```
config dnsfilter profile
  edit { name }
  # Configure DNS domain filter profiles.
  set name { string } Profile name. size[35]
  set comment { string } Comment. size[255]
  set domain-filter-table { integer } DNS domain filter table ID. range[0-4294967295] - datasource(s): dnsfilter.domain-filter.id
  set options { error-allow | ftgd-disable } FortiGuard DNS filter options.
    error-allow Allow all domains when FortiGuard DNS servers fail.
    ftgd-disable Disable FortiGuard DNS domain rating.
  config filters
    edit { id }
    # FortiGuard DNS domain filters.
    set id { integer } ID number. range[0-255]
    set category { integer } Category number. range[0-255]
    set action { block | monitor } Action to take for DNS requests matching the category.
      block Block DNS requests matching the category.
      monitor Allow DNS requests matching the category and log the result.
    set log { enable | disable } Enable/disable DNS filter logging for this DNS profile.
  next
  set log-all-domain { enable | disable } Enable/disable logging of all domains visited (detailed DNS logging).
  set sdns-ftgd-err-log { enable | disable } Enable/disable FortiGuard SDNS rating error logging.
  set sdns-domain-log { enable | disable } Enable/disable domain filtering and botnet domain logging.
  set block-action { block | redirect } Action to take for blocked domains.
    block Return NXDOMAIN for blocked domains.
    redirect Redirect blocked domains to SDNS portal.
  set redirect-portal { ipv4 address } IP address of the SDNS redirect portal.
  set block-botnet { disable | enable } Enable/disable blocking botnet C&C DNS lookups.
  set safe-search { disable | enable } Enable/disable Google, Bing, and YouTube safe search.
  set youtube-restrict { strict | moderate } Set safe search for YouTube restriction level.
    strict Enable strict safe search for YouTube.
    moderate Enable moderate safe search for YouTube.
  next
end
```


endpoint-control

Use endpoint-control commands to configure the following parts of the Endpoint NAC feature:

- Endpoint license registration synchronization
- Endpoint NAC profiles
- the required minimum version of FortiClient Endpoint Security
- the FortiClient installer download location

Endpoint NAC is enabled in firewall policies.

This section includes syntax for the following commands:

- `endpoint-control client`
- `endpoint-control forticlient-registration-sync`
- `endpoint-control profile`
- `endpoint-control registered-forticlient`
- `endpoint-control settings`

endpoint-control client

Introduction.

```
config endpoint-control client
  edit { id }
  # Configure endpoint control client lists.
  set id { integer }   Endpoint client ID. range[0-4294967295]
  set ftcl-uid { string }   Endpoint FortiClient UID. size[32]
  set src-ip { ipv4 address any }   Endpoint client IP address.
  set src-mac { mac address }   Endpoint client MAC address.
  set info { string }   Endpoint client information.
  set ad-groups { string }   Endpoint client AD logon groups. size[51299]
next
end
```

endpoint-control forticlient-registration-sync

Introduction.

```
config endpoint-control forticlient-registration-sync
  edit { peer-name }
  # Configure FortiClient registration synchronization settings.
  set peer-name { string } Peer name. size[35]
  set peer-ip { ipv4 address } IP address of the peer FortiGate for endpoint license synchronization.
  next
end
```

endpoint-control profile

Introduction.

```

config endpoint-control profile
  edit { profile-name }
  # Configure FortiClient endpoint control profiles.
  set profile-name { string } Profile name. size[35]
  set forticlient-registration-compliance-action { block | warning } FortiClient registration compliance action.
    block Block access for devices that are operating without a registered version of FortiClient.
    warning Display a warning for devices that are operating without a registered version of FortiClient.
  set forticlient-security-posture { enable | disable } Enable/disable FortiClient security posture check options.
  set forticlient-security-posture-compliance-action { block | warning } FortiClient security posture compliance action.
    block Block devices that fail FortiClient security posture checking.
    warning Warn devices that fail FortiClient security posture checking.
  set forticlient-av { enable | disable } Enable/disable FortiClient AntiVirus scanning.
  set av-realttime-protection { enable | disable } Enable/disable FortiClient AntiVirus real-time protection.
  set av-signature-up-to-date { enable | disable } Enable/disable FortiClient AV signature updates.
  set sandbox-analysis { enable | disable } Enable/disable sending files to FortiSandbox for analysis.
  set sandbox-address { string } FortiSandbox address. size[255]
  set os-av-software-installed { enable | disable } Enable/disable checking for OS recognized AntiVirus software.
  set forticlient-application-firewall { enable | disable } Enable/disable the FortiClient application firewall.
  set forticlient-application-firewall-list { string } FortiClient application firewall rule list. size[35] - datasource(s): applic-
ation.list.name
  set forticlient-wf { enable | disable } Enable/disable FortiClient web filtering.
  set forticlient-wf-profile { string } The FortiClient web filter profile to apply. size[35] - datasource(s): webfilter.profile.name
  set forticlient-system-compliance { enable | disable } Enable/disable enforcement of FortiClient system compliance.
  set forticlient-system-compliance-action { block | warning } Block or warn clients not compliant with FortiClient requirements.
    block Block clients not in compliance with FortiClient requirements.
    warning Warn clients not in compliance with FortiClient requirements.
  set forticlient-minimum-software-version { enable | disable } Enable/disable requiring clients to run FortiClient with a minimum soft-
ware version number.
  set forticlient-win-ver { string } Minimum FortiClient Windows version. size[63]
  set forticlient-mac-ver { string } Minimum FortiClient Mac OS version. size[63]
  config forticlient-operating-system
    edit { id }
    # FortiClient operating system.
    set id { integer } Operating system entry ID. range[0-4294967295]
    set os-type { option } Operating system type.

```

```

        custom          Customize OS.
        mac_os          Mac OS.
        win_7           Windows 7.
        win_80          Windows 8.0.
        win_81          Windows 8.1.
        win_10          Windows 10.
        win_2000        Windows 2000.
        win_home_svr    Windows Home Server.
        win_svr_10      Windows Server 10.
        win_svr_2003    Windows Server 2003.
        win_svr_2003_r2 Windows Server 2003 R2.
        win_svr_2008    Windows Server 2008.
        win_svr_2008_r2 Windows Server 2008 R2.
        win_svr_2012    Windows Server 2012.
        win_svr_2012_r2 Windows Server 2012 R2.
        win_sto_svr_2003 Windows Storage Server 2003.
        win_vista       Windows Vista.
        win_xp          Windows XP.
    set os-name { string } Customize operating system name or Mac OS format:x.x.x size[127]
next
config forticlient-running-app
edit { id }
    # Use FortiClient to verify if the listed applications are running on the client.
    set id { integer } Application ID. range[0-4294967295]
    set app-name { string } Application name. size[127]
    set process-name { string } Process name. size[127]
    set app-sha256-signature { string } App's SHA256 signature. size[64]
    set process-name2 { string } Process name. size[127]
    set app-sha256-signature2 { string } App's SHA256 Signature. size[64]
    set process-name3 { string } Process name. size[127]
    set app-sha256-signature3 { string } App's SHA256 Signature. size[64]
    set process-name4 { string } Process name. size[127]
    set app-sha256-signature4 { string } App's SHA256 Signature. size[64]
next
config forticlient-registry-entry
edit { id }
    # FortiClient registry entry.
    set id { integer } Registry entry ID. range[0-4294967295]
    set registry-entry { string } Registry entry. size[127]
next
config forticlient-own-file
edit { id }
    # Checking the path and filename of the FortiClient application.

```

```

        set id { integer }   File ID. range[0-4294967295]
        set file { string }  File path and name. size[127]
    next
set forticlient-log-upload { enable | disable }  Enable/disable uploading FortiClient logs.
set forticlient-log-upload-level { traffic | vulnerability | event }  Select the FortiClient logs to upload.
    traffic      Upload traffic logs.
    vulnerability Upload vulnerability logs.
    event        Upload event logs.
set forticlient-log-upload-server { string }  IP address or FQDN of the server to which to upload FortiClient logs. size[255]
set forticlient-vuln-scan { enable | disable }  Enable/disable FortiClient vulnerability scanning.
set forticlient-vuln-scan-compliance-action { block | warning }  FortiClient vulnerability compliance action.
    block  Block clients if FortiClient vulnerability scanning finds a vulnerability.
    warning Create a warning if FortiClient vulnerability scanning finds a vulnerability.
set forticlient-vuln-scan-enforce { option }  Configure the level of the vulnerability found that causes a FortiClient vulnerability compliance action.
    critical Finding a critical-level vulnerability causes a FortiClient compliance action.
    high      Finding a high-level vulnerability causes a FortiClient compliance action.
    medium    Finding a medium-level vulnerability causes a FortiClient compliance action.
    low       Finding a low-level vulnerability causes a FortiClient compliance action.
    info      Finding an info-level vulnerability causes a FortiClient compliance action.
set forticlient-vuln-scan-enforce-grace { integer }  FortiClient vulnerability scan enforcement grace period (0 - 30 days, default = 1).
range[0-30]
set forticlient-vuln-scan-exempt { enable | disable }  Enable/disable compliance exemption for vulnerabilities that cannot be patched automatically.
set forticlient-wf { enable | disable }  Enable/disable FortiClient web filtering.
set forticlient-wf-profile { string }  The FortiClient web filter profile to apply. size[35] - datasource(s): webfilter.profile.name
set disable-wf-when-protected { enable | disable }  Enable/disable FortiClient web category filtering when protected by FortiGate.
set forticlient-vpn-provisioning { enable | disable }  Enable/disable FortiClient VPN provisioning.
set forticlient-advanced-vpn { enable | disable }  Enable/disable advanced FortiClient VPN configuration.
set forticlient-advanced-vpn-buffer { string }  Advanced FortiClient VPN configuration. size[32768]
config forticlient-vpn-settings
edit { name }
# FortiClient VPN settings.
    set name { string }  VPN name. size[35]
    set type { ipsec | ssl }  VPN type (IPsec or SSL VPN).
        ipsec  IPsec VPN.
        ssl    SSL VPN.
    set remote-gw { string }  IP address or FQDN of the remote VPN gateway. size[255]
    set sslvpn-access-port { integer }  SSL VPN access port (1 - 65535). range[1-65535]
    set sslvpn-require-certificate { enable | disable }  Enable/disable requiring SSL VPN client certificate.
    set auth-method { psk | certificate }  Authentication method.
        psk          Pre-shared key.
        certificate  Certificate.

```

```

        set preshared-key { password_string } Pre-shared secret for PSK authentication. size[128]
    next
set forticlient-wf { enable | disable } Enable/disable FortiClient web filtering.
set forticlient-wf-profile { string } The FortiClient web filter profile to apply. size[35] - datasource(s): webfilter.profile.name
set disable-wf-when-protected { enable | disable } Enable/disable FortiClient web category filtering when protected by FortiGate.
set client-vpn-provisioning { enable | disable } FortiClient VPN provisioning.
config client-vpn-settings
    edit { name }
    # FortiClient VPN settings.
    set name { string } VPN name. size[35]
    set type { ipsec | ssl } VPN type (IPsec or SSL VPN).
        ipsec IPsec VPN.
        ssl SSL VPN.
    set vpn-configuration-name { string } Name of VPN configuration. size[35]
    set vpn-configuration-content { string } Content of VPN configuration. size[32768]
    set remote-gw { string } IP address or FQDN of the remote VPN gateway. size[255]
    set sslvpn-access-port { integer } SSL VPN access port (1 - 65535). range[1-65535]
    set sslvpn-require-certificate { enable | disable } Enable/disable requiring SSL VPN client certificate.
    set auth-method { psk | certificate } Authentication method.
        psk Pre-shared key.
        certificate Certificate.
    set preshared-key { password_string } Pre-shared secret for PSK authentication. size[128]
    next
set distribute-configuration-profile { enable | disable } Enable/disable configuration profile (.mobileconfig file) distribution.
set configuration-name { string } Name of configuration profile. size[35]
set configuration-content { string } Content of configuration profile. size[32768]
set description { string } Description. size[255]
config src-addr
    edit { name }
    # Source addresses.
    set name { string } Address object from available options. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
config device-groups
    edit { name }
    # Device groups.
    set name { string } Device group object from available options. size[64] - datasource(s): user.device-group.name,user.device-cat-
egory.name
    next
config users
    edit { name }
    # Users.
    set name { string } User name. size[64] - datasource(s): user.local.name
    next

```

```
config user-groups
  edit { name }
  # User groups.
  set name { string }  User group name. size[64] - datasource(s): user.group.name
  next
config on-net-addr
  edit { name }
  # Addresses for on-net detection.
  set name { string }  Address object from available options. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  set replacemsg-override-group { string }  Select an endpoint control replacement message override group from available options. size[35] -
datasource(s): system.replacemsg-group.name
  next
end
```


endpoint-control registered-forticlient

Introduction.

```
config endpoint-control registered-forticlient
  edit { uid }
    # Registered FortiClient list.
    set uid { string } FortiClient UID. size[32]
    set vdom { string } Registering vdom. size[31]
    set ip { ipv4 address any } Endpoint IP address.
    set mac { mac address } Endpoint MAC address.
    set status { integer } FortiClient registration status. range[0-65535]
    set flag { integer } FortiClient registration flag. range[0-65535]
    set reg-fortigate { string } Registering FortiGate SN. size[19]
  next
end
```

endpoint-control settings

Introduction.

```
config endpoint-control settings
  set forticlient-reg-key-enforce { enable | disable }  Enable/disable requiring or enforcing FortiClient registration keys.
  set forticlient-reg-key { password_string }  FortiClient registration key. size[128]
  set forticlient-reg-timeout { integer }  FortiClient registration license timeout (days, min = 1, max = 180, 0 means unlimited). range[0-180]
  set download-custom-link { string }  Customized URL for downloading FortiClient. size[127]
  set download-location { fortiguard | custom }  FortiClient download location (FortiGuard or custom).
    fortiguard  You can download FortiClient from FortiGuard.
    custom      Specify a custom location for downloading FortiClient. Used when you can't access FortiGuard.
  set forticlient-keepalive-interval { integer }  Interval between two KeepAlive messages from FortiClient (20 - 300 sec, default = 60). range[20-300]
  set forticlient-sys-update-interval { integer }  Interval between two system update messages from FortiClient (30 - 1440 min, default = 720). range[30-1440]
  set forticlient-avdb-update-interval { integer }  Period of time between FortiClient AntiVirus database updates (0 - 24 hours, default = 8). range[0-24]
  set forticlient-warning-interval { integer }  Period of time between FortiClient portal warnings (0 - 24 hours, default = 1). range[0-24]
  set forticlient-user-avatar { enable | disable }  Enable/disable uploading FortiClient user avatars.
end
```

extender-controller

Use this command to configure .

This section includes syntax for the following commands:

- `extender-controller extender`

extender-controller extender

Introduction.

```
config extender-controller extender
  edit { id }
  # Extender controller configuration.
  set id { string } FortiExtender serial number. size[19]
  set admin { disable | discovered | enable } FortiExtender Administration (enable or disable).
  set ifname { string } FortiExtender interface name. size[15]
  set vdom { integer } VDOM range[0-4294967295]
  set role { none | primary | secondary } FortiExtender work role(Primary, Secondary, None).
    none FortiExtender is not supplying any service.
    primary FortiExtender is supplying primary service.
    secondary FortiExtender is standby for primary FortiExtender.
  set mode { standalone | redundant } FortiExtender mode.
    standalone Standalone.
    redundant Redundant for an interface.
  set dial-mode { dial-on-demand | always-connect } Dial mode (dial-on-demand or always-connect).
    dial-on-demand The dial action is controlled by user.
    always-connect auto dial.
  set redial { option } Number of redials allowed based on failed attempts.
    none Forever.
    1 One attempt.
    2 Two attempts.
    3 Three attempts.
    4 Four attempts.
    5 Five attempts.
    6 Six attempts.
    7 Seven attempts.
    8 Eight attempts.
    9 Nine attempts.
    10 Ten attempts.
  set redundant-intf { string } Redundant interface. size[15]
  set dial-status { integer } Dial status. range[0-4294967295]
  set conn-status { integer } Connection status. range[0-4294967295]
  set ext-name { string } FortiExtender name. size[31]
  set description { string } Description. size[31]
  set quota-limit-mb { integer } Monthly quota limit (MB). range[0-10485760]
```

```
set billing-start-day { integer } Billing start day. range[1-28]
set at-dial-script { string } Initialization AT commands specific to the MODEM. size[127]
set modem-passwd { password_string } MODEM password. size[27]
set initiated-update { enable | disable } Allow/disallow network initiated updates to the MODEM.
set modem-type { cdma | gsm/lte | wimax } MODEM type (CDMA, GSM/LTE or WIMAX).
    cdma    CDMA
    gsm/lte GSM/LTE
    wimax   WIMAX
set ppp-username { string } PPP username. size[31]
set ppp-password { password_string } PPP password. size[27]
set ppp-auth-protocol { auto | pap | chap } PPP authentication protocol (PAP,CHAP or auto).
    auto   AUTO
    pap    PAP
    chap   CHAP
set ppp-echo-request { enable | disable } Enable/disable PPP echo request.
set wimax-carrier { string } WiMax carrier. size[31]
set wimax-realm { string } WiMax realm. size[31]
set wimax-auth-protocol { tls | ttls } WiMax authentication protocol(TLS or TTLS).
    tls    TLS
    ttls   TTLS
set sim-pin { password_string } SIM PIN. size[27]
set access-point-name { string } Access point name(APN). size[63]
set multi-mode { option } MODEM mode of operation(3G,LTE,etc).
    auto      AUTO
    auto-3g   Auto 3G(3G or less)
    force-lte Force LTE
    force-3g  Force 3G
    force-2g  Force 2G
set roaming { enable | disable } Enable/disable MODEM roaming.
set cdma-nai { string } NAI for CDMA MODEMS. size[31]
set aaa-shared-secret { password_string } AAA shared secret. size[27]
set ha-shared-secret { password_string } HA shared secret. size[27]
set primary-ha { string } Primary HA. size[31]
set secondary-ha { string } Secondary HA. size[31]
set cdma-aaa-spi { string } CDMA AAA SPI. size[31]
set cdma-ha-spi { string } CDMA HA SPI. size[31]
next
end
```

firewall

Use firewall commands to configure firewall policies and the data they use.

This section includes syntax for the following commands:

- `firewall acl | acl6`
- `firewall address | address6`
- `firewall addrgrp | addgrp6`
- `firewall auth-portal`
- `firewall central-snat-map`
- `firewall dnstranslation`
- `firewall DoS-policy | DoS-policy6`
- `firewall identity-based-route`
- `firewall interface-policy | interface-policy6`
- `firewall internet-service`
- `firewall internet-service-custom`
- `firewall ipmacbinding setting`
- `firewall ipmacbinding table`
- `firewall ippool | ippool6`
- `firewall ip-translation`
- `firewall ipv6-eh-filter`
- `firewall ldb-monitor`
- `firewall local-in-policy | local-in-policy6`
- `firewall multicast-address | multicast-address6`
- `firewall multicast-policy | multicast-policy6`
- `firewall policy | policy6`
- `firewall policy46 | policy64`
- `firewall profile-group`
- `firewall profile-protocol-options`

- firewall proxy-address
- firewall proxy-addrgrp
- firewall proxy-policy
- firewall schedule group
- firewall schedule onetime
- firewall schedule recurring
- firewall service category
- firewall service custom
- firewall service group
- firewall shaper per-ip-shaper
- firewall shaper traffic-shaper
- firewall shaping-policy
- firewall sniffer
- firewall ssl setting
- firewall ssl-server
- firewall ssl-ssh-profile
- firewall ttl-policy
- firewall vip | vip6
- firewall vip46 | vip64
- firewall vipgrp | vipgrp6
- firewall vipgrp46 | vipgrp64

firewall {acl | acl6}

Introduction.

```
config firewall acl
  edit { policyid }
  # Configure IPv4 access control list.
  set policyid { integer }  Policy ID. range[0-9999]
  set status { enable | disable }  Enable/disable access control list status.
  set comments { string }  Comment. size[1023]
  set interface { string }  Interface name. size[35] - datasource(s): system.zone.name,system.interface.name
  config srcaddr
    edit { name }
    # Source address name.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstaddr
    edit { name }
    # Destination address name.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config service
    edit { name }
    # Service name.
    set name { string }  Address name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
next
end

config firewall acl6
  edit { policyid }
  # Configure IPv6 access control list.
  set policyid { integer }  Policy ID. range[0-9999]
  set status { enable | disable }  Enable/disable access control list status.
  set comments { string }  Comment. size[1023]
  set interface { string }  Interface name. size[35] - datasource(s): system.zone.name,system.interface.name
  config srcaddr
```



```
        edit { name }
        # Source address name.
        set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
        next
    config dstaddr
        edit { name }
        # Destination address name.
        set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
        next
    config service
        edit { name }
        # Service name.
        set name { string } Address name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
        next
    next
end
```

firewall {address | address6}

Use this command to configure firewall addresses used in firewall policies. An IPv4 firewall address is a set of one or more IP addresses, represented as a domain name, an IP address and a subnet mask, or an IP address range. An IPv6 firewall address is an IPv6 address prefix. Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies. If an address is selected in a policy, it cannot be deleted until it is deselected from the policy.

```
config firewall address
  edit { name }
  # Configure IPv4 addresses.
  set name { string }   Address name. size[63]
  set uuid { uuid }     Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set subnet { ipv4 classnet any }   IP address and subnet mask of address.
  set type { option }   Type of address.
    ipmask              Standard IPv4 address with subnet mask.
    iprange             Range of IPv4 addresses between two specified addresses (inclusive).
    fqdn                Fully Qualified Domain Name address.
    geography           IP addresses from a specified country.
    wildcard            Standard IPv4 using a wildcard subnet mask.
    wildcard-fqdn      Fully Qualified Domain Name with wildcard characters.
  set start-ip { ipv4 address any }   First IP address (inclusive) in the range for the address.
  set end-ip { ipv4 address any }     Final IP address (inclusive) in the range for the address.
  set fqdn { string }                Fully Qualified Domain Name address. size[255]
  set country { string }             IP addresses associated to a specific country. size[2]
  set wildcard-fqdn { string }       Fully Qualified Domain Name with wildcard characters. size[255]
  set cache-ttl { integer }          Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds. range[0-86400]
  set wildcard { ipv4 classnet any } IP address and wildcard netmask.
  set comment { string }            Comment. size[255]
  set visibility { enable | disable } Enable/disable address visibility in the GUI.
  set associated-interface { string } Network interface associated with address. size[35] - datasource(s): system.interface.name,system.zone.name
  set color { integer }             Color of icon on the GUI. range[0-32]
  config tags
    edit { name }
    # Names of object-tags applied to address.
    set name { string }            Tag name. size[64] - datasource(s): system.object-tag.name
    next
  set allow-routing { enable | disable } Enable/disable use of this address in the static route configuration.
```

```

    next
end

config firewall address6
    edit { name }
    # Configure IPv6 firewall addresses.
    set name { string }    Address name. size[63]
    set uuid { uuid }     Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
    set type { ipprefix | iprange }    Type of IPv6 address object (default = ipprefix).
        ipprefix    Uses the IP prefix to define a range of IPv6 addresses.
        iprange     Range of IPv6 addresses between two specified addresses (inclusive).
    set ip6 { ipv6 network }    IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).
    set start-ip { ipv6 address }    First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).
    set end-ip { ipv6 address }    Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).
    set visibility { enable | disable }    Enable/disable the visibility of the object in the GUI.
    set color { integer }    Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).
range[0-32]
    config tags
        edit { name }
        # Names of object-tags applied to address. Tags need to be preconfigured in config system object-tag. Separate multiple tags with a
space.
            set name { string }    Tag name. size[64] - datasource(s): system.object-tag.name
        next
    set comment { string }    Comment. size[255]
    next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

Syntax

```

config firewall {address | address6}
    {edit|delete|rename|get|show} <name_str>

```

Managing address objects

The configuration of specific address object is the most common activity when using the config firewall address command but some commands affect the address objects as a whole.

edit

Used to select which individual address object to configure or edit values.

```
edit <address_name>
```

To get a list of all of the existing address objects, type the command:

```
Command Prompt (address) # edit ?
```

or

```
Command Prompt (address6) # edit ?
```

If you are creating a new address object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

delete

Used to delete an existing address object

```
delete <address_name>
```

- The <address_name> can be a string of up to 64 characters.

purge

Used to delete all of the existing address or address6 objects. It deletes all of the values within the table that holds the information about address or address6 objects within the VDOM.

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

rename

Used to change the name of the address object.

```
rename <address_name> to <new_address_name>
```

name

This field is a unique name given to represent the address object. This setting is for both IPv4 and IPv6. This setting is first defined when using the edit command to edit an address object that does not currently exist. This setting is available for both `address` and `address6`. The name field of an address object cannot be changed from within the object. It can be changed by using the rename command in the `config firewall address` or `config firewall address6` context.

uuid

Each address has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited. This setting is available for both `address` and `address6`.

Syntax:

```
set uuid <uuid>
```

Default value: autogenerated

Example:

```
config firewall address
  edit example.com
    set uuid d38e0dca-b80c-51e6-1180-6863e1b9ea9a
end
```

subnet

The IP address and subnet mask of the address. By using different subnet masks a single IP address can be defined or a group of addresses. This setting is only available for `address`. This option is available only if the `type` option is set to `ipmask`.

Syntax:

```
set subnet <ipv4-classnet-any>
```

Default value: 0.0.0.0 0.0.0.0

Example:

```
config firewall address
  edit example.com
  set type ipmask
  set subnet 192.168.1.1 255.255.255.255
  or ...
  set subnet 192.168.1.1/32
end
```

type

This field sets the type of address object. There are two sets of types for addresses. The first is for IPv4 addresses the second is for IPv6.

IPv4 types

- `ipmask` - a standard IPv4 address with subnet mask
- `iprange` - a range of IPv4 addresses between two specified addresses (inclusive).
- `fqdn` - a Fully Qualified Domain Name address
- `geography` - IP addresses from a specified country
- `wildcard` - a standard IPv4 using a wildcard subnet mask
- `wildcard-fqdn` - a Fully Qualified Domain Name with wildcard characters

IPv6 types

- `ipprefix` - uses the IP prefix to define a range of IPv6 addresses
- `iprange` - a range of IPv6 addresses between two specified addresses (inclusive).

Syntax:

```
set type {ipmask | iprange | fqdn | geography | wildcard | wildcard-fqdn}
```

Default value: `ipmask` or

```
set type {ipprefix | iprange}
```

Default value: `ipprefix`

Example:

```
config firewall address
    edit example.com
        set type ipmask
    end
```

ip6

This is for the IPv6 address prefix. This setting is only available for `address6`.

Syntax:

```
set ip6 <ipv6-network>
```

Default value: `::/0`

Example:

```
config firewall address6
    edit example.com
        set ip6 2001:db8:a0b:12f0::1/64
    end
```

start-ip

The first IP address (inclusive) in the range for the address. This setting is available for both `address` and `address6`. This option is available only if the `type` option is set to `iprange`.

Syntax:

```
set start-ip <ipv4-address-any>
```

Default value: `0.0.0.0 0.0.0.0` or

```
set start-ip <ipv6-address>
```

Default value: `::`

Example:

```
config firewall address
  edit example.com
  set type iprange
  set start-ip 192.168.1.43
  or ...
  config firewall address6
  edit example.com
  set type iprange
set start-ip 2001:db8:a0b:12f0::1
```

end-ip

The final IP address (inclusive) in the range for the address. This setting is available for both `address` and `address6`. This option is available only if the `type` option is set to `iprange`.

Syntax:

```
set end-ip <ipv4-address-any>
```

Default value: 0.0.0.0 0.0.0.0 or

```
set end-ip <ipv6-address>
```

Default value: ::

Example:

```
config firewall address
  edit example.com
  set type iprange
  set end-ip 192.168.1.201
  or ...
  config firewall address6
  edit example.com
  set type iprange
set end-ip 2001:db8:a0b:12f0::89
```


fqdn

This setting defines a Fully qualified domain name which is normally translated to an IP address by a DNS server. This setting is only available for `address`. This option is available only if the `type` option is set to `fqdn`.

Syntax:

```
set fqdn <string>
```

Example:

```
config firewall address
  edit example.com
  set type fqdn
  set fqdn example.com
end
```

country

This field is used to set the country and all of its IP addresses. This setting is only available for `address`. This option is available only if the `type` option is set to `geography`. The options in this field are 2 character country code that represent different countries or other options. To get a listing type the command `set country ?`. An example of some of the available options are:

```
ZZ    Reserved
A1    Anonymous Proxy
A2    Satellite Provider
O1    Other Country
AD    Andorra
.
.
.
ZW    Zimbabwe
```

Syntax:

```
set country <2 character string>
```

Example:

```
config firewall address
  edit example.com
  set type geography
  set country US
end
```

wildcard-fqdn

A Fully Qualified Domain Name, but using wildcard symbols in place of some of the characters. This setting is only available for `address`. This option is available only if the `type` option is set to `wildcard-fqdn`.

Syntax:

```
set wildcard-fqdn <string>
```

Example:

```
config firewall address
  edit example.com
  set wildcard-fqdn *.example.com
end
```

cache-ttl

This setting defines the minimal TTL (time to live) of individual IP addresses in FQDN cache. The TTL is measured in seconds. This setting is only available for `address`. This option is available only if the `type` option is set to `fqdn`.

Syntax:

```
set cache-ttl <integer>
```

Default value: 0 **Example:**

```
config firewall address
  edit example.com
```

```
set cache-ttl 3600
```

wildcard

This setting defines an IP address and a wildcard netmask. This setting is only available for `address`. This option is available only if the `type` option is set to `wildcard`.

Syntax:

```
set wildcard <ipv4-classnet-any>
```

Default value: 0.0.0.0 0.0.0.0

Example:

```
config firewall address
  edit example.com
    set wildcard 192.168.0.0 255.255.0.64
end
```

comment

Field used to store descriptive information about the address. The field is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces. This setting is available for both `address` and `address6`.

Syntax:

```
set comment <var-string>
```

Example:

```
config firewall address
  edit example.com
    set comment "Address for the Example Company website"
end
```

visibility

Enables or disables the ability to see the address in the GUI. This setting is available for both `address` and `address6`.

Syntax:

```
set visibility {enable | disable}
```

Default value: `enable`

Example:

```
config firewall address
  edit example.com
    set visibility disable
end
```

associated-interface

Use this option to associate the address to a specific interface on the FortiGate. The address will only be available for selection if the associated interface is associated to the policy. The option to choose any interface is also available. This setting is only available for `address`.

Syntax:

```
set associated-interface <string>
```

Example:

```
config firewall address
  edit example.com
    set associated-interface wan1
end
```

color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1. This setting is available for both `address` and `address6`.

Syntax:

```
set color <integer>
```

Default value: 0

Example:

```
config firewall address
  edit example.com
    set color 15
end
```

tags

Used to assign a custom tag to the address object. The tags need to be preconfigured in `config system object-tag` and the same list of tags can be used anywhere that the tag setting is available. To see what tags are available for use, use the command `set tags ?`. This setting is available for both `address` and `address6`. Separate multiple values with a space.

Syntax:

```
{set|append|clear} tags <name_of_tag>
```

Example:

```
config system object-tag
  edit example-tag1
  next
  edit example-tag2
  next
  edit "example tag 3"
```

```
        next
    end

    config firewall address
        edit example.com
            set tags example-tag1 example-tag2
            append "example tag 3"
        end
    end
```

allow-routing

Enable/disable use of this address in the static route configuration. This setting is only available for `address`.

Syntax:

```
set allow-routing {enable | disable}
```

Default value: `disable`

Example:

```
config firewall address
    edit example.com
        set allow-routing enable
    end
```

firewall {addrgrp | addgrp6}

Use this command to configure firewall address groups used in firewall policies. You can organize related firewall addresses into firewall address groups to simplify firewall policy configuration. For example, rather than creating three separate firewall policies for three firewall addresses, you could create a firewall address group consisting of the three firewall addresses, then create one firewall policy using that firewall address group. Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies. If an address group is selected in a policy, it cannot be deleted unless it is first deselected in the policy. An address group can be a member of another address group.

```
config firewall addrgrp
  edit { name }
  # Configure IPv4 address groups.
  set name { string }   Address group name. size[63]
  set uuid { uuid }    Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  config member
    edit { name }
    # Address objects contained within the group.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  set comment { string }  Comment. size[255]
  set visibility { enable | disable }  Enable/disable address visibility in the GUI.
  set color { integer }   Color of icon on the GUI. range[0-32]
  config tags
    edit { name }
    # Name(s) of object-tags applied to address.
    set name { string }   Tag name. size[64] - datasource(s): system.object-tag.name
    next
  set allow-routing { enable | disable }  Enable/disable use of this group in the static route configuration.
next
end

config firewall addrgrp6
  edit { name }
  # Configure IPv6 address groups.
  set name { string }   IPv6 address group name. size[63]
  set uuid { uuid }    Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set visibility { enable | disable }  Enable/disable address group6 visibility in the GUI.
  set color { integer }  Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets the value to 1). range
```

```
[0-32]
set comment { string } Comment. size[255]
config member
edit { name }
# Address objects contained within the group.
set name { string } Address6/addrgrp6 name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
next
config tags
edit { name }
# Names of object-tags applied to address. Tags need to be preconfigured in config system object-tag. Separate multiple tags with a
space.
set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
next
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

Syntax

```
config firewall {addrgrp | addrgrp6}
{edit|delete|purge|rename|get|show} <name_str>
```

Managing address objects

The configuration of specific address object is the most common activity when using the config firewall address command but some commands affect the address objects as a whole.

edit

Used to select which individual policy to configure or edit values.

```
edit <address_group>
```

To get a list of all of the existing address objects, type the command:


```
Command Prompt (addrgrp) # edit ?  
or  
Command Prompt (addrgrp6) # edit ?
```

If you are creating a new address object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

delete

Used to delete an existing address object

```
delete <address_group>
```

- The <address_group> can be a string of up to 64 characters.

purge

Used to delete all of the existing `addrgrp` or `addrgrp6` objects. It deletes all of the values within the table that holds the information about `addrgrp` or `addrgrp6` objects within the VDOM.

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

rename

Used to change the name of the `addrgrp` or `addrgrp6` object.

```
rename <address_group> to <new_address_group>
```

name

This field is a unique name given to represent the address group object. This setting is for both IPv4 and IPv6. This setting is first defined when using the `edit` command to edit an address group object that does not currently exist. The name field of an address object cannot be changed from within the object. It can be changed by using the `rename` command in the `config firewall addrgrp` or `config firewall addrgrp6` context.

uuid

Each address has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited. This settings is for both IPv4 and IPv6.

Syntax:

```
set uuid <uuid>
```

Default value: autogenerated

Example:

```
config firewall addrgrp
  edit example_group
    set uuid d38e0dca-b80c-51e6-1180-6863e1b9ea9a
end
```

member

Defines the address objects that are members of the address group. The value is a <string> that should be the name of one of the existing address objects configured on the device. A group cannot contain both IPv4 and IPv6 address objects. Separate multiple interfaces with a space.

Syntax:

```
{set|append} members <name of address object> [<name of address object> ...]
```

Example:

```
config firewall addrgrp
  edit example_group
    set member example_address1
  or ...
  set member example_address1 example_address2
  or ...
  append example_address3
end
```

comment

Field used to store descriptive information about the address group. The field is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces. This settings is for both IPv4 and IPv6.

Syntax:

```
set comment <var-string>
```

Example:

```
config firewall addrgrp
    edit example.com
        set comment "Addresses for Vendor Websites"
    end
```

visibility

Enables or disables the ability to see the address group in the GUI. This settings is for both IPv4 and IPv6.

Syntax:

```
set visibility {enable | disable}
```

Default value: enable

Example:

```
config firewall addrgrp
    edit example_group
        set visibility disable
    end
```

color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1. This settings is for both IPv4 and IPv6.

Syntax:

```
set color <integer>
```

Default value: 0**Example:**

```
config firewall addrgrp
    edit example_group
        set color 7
end
```

tags

Used to assign a custom tag to the address group object. The tags need to be preconfigured in `config system object-tag` and the same list of tags can be used anywhere that the tag setting is available. To see what tags are available for use, use the command `set tags ?`. This settings is for both IPv4 and IPv6. Separate multiple values with a space.

Syntax:

```
{set|append|clear} tags <name_of_tag>
```

Example:

```
config system object-tag
    edit example-tag1
    next
    edit example-tag2
    next
    edit "example tag 3"
    next
end

config firewall addrgrp
    edit example_group
    set tags example-tag1 example-tag2
```

```
        append "example tag 3"  
end
```

allow-routing

Enable/disable use of this address group in the static route configuration. This option is only available for IPv4.

Syntax:

```
set allow-routing {enable | disable}
```

Default value: disable

Example:

```
config firewall addrgrp  
    edit example_group  
        set allow-routing enable  
end
```

firewall auth-portal

Introduction.

```
config firewall auth-portal
  config groups
    edit { name }
      # Firewall user groups permitted to authenticate through this portal. Separate group names with spaces.
      set name { string }  Group name. size[64] - datasource(s): user.group.name
    next
  set portal-addr { string }  Address (or FQDN) of the authentication portal.. size[63]
  set portal-addr6 { string }  IPv6 address (or FQDN) of authentication portal. size[63]
  set identity-based-route { string }  Name of the identity-based route that applies to this portal. size[35] - datasource(s): firewall.identity-
based-route.name
end
```

firewall central-snat-map

Introduction.

```
config firewall central-snat-map
  edit { policyid }
  # Configure central SNAT policies.
  set policyid { integer } Policy ID. range[0-4294967295]
  set status { enable | disable } Enable/disable the active status of this policy.
  config orig-addr
    edit { name }
    # Original address.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config srcintf
    edit { name }
    # Source interface name from available interfaces.
    set name { string } Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
  config dst-addr
    edit { name }
    # Destination address name from available addresses.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstintf
    edit { name }
    # Destination interface name from available interfaces.
    set name { string } Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
  config nat-ippool
    edit { name }
    # Name of the IP pools to be used to translate addresses from available IP Pools.
    set name { string } IP pool name. size[64] - datasource(s): firewall.ippool.name
  next
  set protocol { integer } Integer value for the protocol type (0 - 255). range[0-255]
  set orig-port { integer } Original TCP port (0 to 65535). range[0-65535]
  set nat-port { string } Translated port or port range (0 to 65535).
  set nat { disable | enable } Enable/disable source NAT.
next
```

firewall central-snat-map

end

firewall dnstranslation

Introduction.

```
config firewall dnstranslation
  edit { id }
  # Configure DNS translation.
  set id { integer } ID. range[0-4294967295]
  set src { ipv4 address } 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.
  set dst { ipv4 address } 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.
  set netmask { ipv4 netmask } If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.
  next
end
```

firewall {DoS-policy | DoS-policy6}

Introduction.

```
config firewall DoS-policy
  edit { policyid }
  # Configure IPv4 DoS policies.
  set policyid { integer }   Policy ID. range[0-9999]
  set status { enable | disable }   Enable/disable this policy.
  set comments { string }   Comment. size[1023]
  set interface { string }   Incoming interface name from available interfaces. size[35] - datasource(s): system.zone.name,system.interface.name
  config srcaddr
    edit { name }
    # Source address name from available addresses.
    set name { string }   Service name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstaddr
    edit { name }
    # Destination address name from available addresses.
    set name { string }   Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config service
    edit { name }
    # Service object from available options.
    set name { string }   Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
  config anomaly
    edit { name }
    # Anomaly name.
    set name { string }   Anomaly name. size[63]
    set status { disable | enable }   Enable/disable the active status of this anomaly sensor.
    set log { enable | disable }   Enable/disable logging for this anomaly.
    set action { pass | block | proxy }   Action taken when the threshold is reached.
      pass Allow traffic but record a log message if logging is enabled.
      block Block traffic if this anomaly is found.
      proxy Use a proxy to control the traffic flow.
    set quarantine { none | attacker }   Quarantine method.
      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.
        set quarantine-expiry { string } Duration of quarantine, from 1 minute to 364 days, 23 hours, and 59 minutes from now. (format:
###d##h##m, default = 5m). Requires quarantine set to attacker.
        set quarantine-log { disable | enable } Enable/disable quarantine logging.
        set threshold { integer } 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. range[1-2147483647]
        set threshold(default) { integer } Anomaly default threshold. range[0-4294967295]
    next
next
end

config firewall DoS-policy6
edit { policyid }
# Configure IPv6 DoS policies.
    set policyid { integer } Policy ID. range[0-9999]
    set status { enable | disable } Enable/disable this policy.
    set comments { string } Comment. size[1023]
    set interface { string } Incoming interface name from available interfaces. size[35] - datasource(s): sys-
tem.zone.name,system.interface.name
    config srcaddr
        edit { name }
        # Source address name from available addresses.
            set name { string } Service name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
        next
    config dstaddr
        edit { name }
        # Destination address name from available addresses.
            set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
        next
    config service
        edit { name }
        # Service object from available options.
            set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
        next
    config anomaly
        edit { name }
        # Anomaly name.
            set name { string } Anomaly name. size[63]
            set status { disable | enable } Enable/disable the active status of this anomaly sensor.
            set log { enable | disable } Enable/disable logging for this anomaly.
            set action { pass | block | proxy } Action taken when the threshold is reached.

```

```
    pass Allow traffic but record a log message if logging is enabled.
    block Block traffic if this anomaly is found.
    proxy Use a proxy to control the traffic flow.
  set quarantine { none | attacker } Quarantine method.
    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.

```
    set quarantine-expiry { string } Duration of quarantine, from 1 minute to 364 days, 23 hours, and 59 minutes from now. (format:
###d##h##m, default = 5m). Requires quarantine set to attacker.
    set quarantine-log { disable | enable } Enable/disable quarantine logging.
    set threshold { integer } 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. range[1-2147483647]
    set threshold(default) { integer } Anomaly default threshold. range[0-4294967295]
  next
next
end
```

firewall identity-based-route

Introduction.

```
config firewall identity-based-route
  edit { name }
  # Configure identity based routing.
  set name { string } Name. size[35]
  set comments { string } Comments. size[127]
  config rule
  edit { id }
  # Rule.
  set id { integer } Rule ID. range[0-4294967295]
  set gateway { ipv4 address } IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx , Default: 0.0.0.0).
  set device { string } Outgoing interface for the rule. size[35] - datasource(s): system.interface.name
  config groups
  edit { name }
  # Select one or more group(s) from available groups that are allowed to use this route. Separate group names with a space.
  set name { string } Group name. size[64] - datasource(s): user.group.name
  next
  next
next
end
```

firewall {interface-policy | interface-policy6}

Introduction.

```
config firewall interface-policy
  edit { policyid }
  # Configure IPv4 interface policies.
  set policyid { integer } Policy ID. range[0-4294967295]
  set status { enable | disable } Enable/disable this policy.
  set comments { string } Comments. size[1023]
  set logtraffic { all | utm | disable } Logging type to be used in this policy (Options: all | utm | disable, Default: utm).
    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.
  set address-type { ipv4 | ipv6 } Policy address type (IPv4 or IPv6).
    ipv4 IPv4.
    ipv6 IPv6.
  set interface { string } Monitored interface name from available interfaces. size[35] - datasource(s): system.zone.name,system.interface.name
  config srcaddr
    edit { name }
    # Address object to limit traffic monitoring to network traffic sent from the specified address or range.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  config dstaddr
    edit { name }
    # Address object to limit traffic monitoring to network traffic sent to the specified address or range.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  config service
    edit { name }
    # Service object from available options.
    set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
    next
  set application-list-status { enable | disable } Enable/disable application control.
  set application-list { string } Application list name. size[35] - datasource(s): application.list.name
  set ips-sensor-status { enable | disable } Enable/disable IPS.
  set ips-sensor { string } IPS sensor name. size[35] - datasource(s): ips.sensor.name
  set dsri { enable | disable } Enable/disable DSRI.
```

```

set av-profile-status { enable | disable } Enable/disable antivirus.
set av-profile { string } Antivirus profile. size[35] - datasource(s): antivirus.profile.name
set webfilter-profile-status { enable | disable } Enable/disable web filtering.
set webfilter-profile { string } Web filter profile. size[35] - datasource(s): webfilter.profile.name
set spamfilter-profile-status { enable | disable } Enable/disable antispam.
set spamfilter-profile { string } Antispam profile. size[35] - datasource(s): spamfilter.profile.name
set dlp-sensor-status { enable | disable } Enable/disable DLP.
set dlp-sensor { string } DLP sensor name. size[35] - datasource(s): dlp.sensor.name
set scan-botnet-connections { disable | block | monitor } Enable/disable scanning for connections to Botnet servers.
    disable Do not scan for connections to botnet servers.
    block Block connections to botnet servers.
    monitor Log connections to botnet servers.
set label { string } Label. size[63]
next
end

config firewall interface-policy6
edit { policyid }
# Configure IPv6 interface policies.
set policyid { integer } Policy ID. range[0-4294967295]
set status { enable | disable } Enable/disable this policy.
set comments { string } Comments. size[1023]
set logtraffic { all | utm | disable } Logging type to be used in this policy (Options: all | utm | disable, Default: utm).
    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.
set address-type { ipv4 | ipv6 } Policy address type (IPv4 or IPv6).
    ipv4 IPv4.
    ipv6 IPv6.
set interface { string } Monitored interface name from available interfaces. size[35] - datasource(s): system.zone.name,system.interface.name
config srcaddr6
edit { name }
# IPv6 address object to limit traffic monitoring to network traffic sent from the specified address or range.
set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
next
config dstaddr6
edit { name }
# IPv6 address object to limit traffic monitoring to network traffic sent to the specified address or range.
set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
next
config service6

```

```
edit { name }
# Service name.
    set name { string }    Address name. size[64] - datasource(s): firewall.service.custom.name, firewall.service.group.name
next
set application-list-status { enable | disable }    Enable/disable application control.
set application-list { string }    Application list name. size[35] - datasource(s): application.list.name
set ips-sensor-status { enable | disable }    Enable/disable IPS.
set ips-sensor { string }    IPS sensor name. size[35] - datasource(s): ips.sensor.name
set dsri { enable | disable }    Enable/disable DSRI.
set av-profile-status { enable | disable }    Enable/disable antivirus.
set av-profile { string }    Antivirus profile. size[35] - datasource(s): antivirus.profile.name
set webfilter-profile-status { enable | disable }    Enable/disable web filtering.
set webfilter-profile { string }    Web filter profile. size[35] - datasource(s): webfilter.profile.name
set spamfilter-profile-status { enable | disable }    Enable/disable antispam.
set spamfilter-profile { string }    Antispam profile. size[35] - datasource(s): spamfilter.profile.name
set dlp-sensor-status { enable | disable }    Enable/disable DLP.
set dlp-sensor { string }    DLP sensor name. size[35] - datasource(s): dlp.sensor.name
set scan-botnet-connections { disable | block | monitor }    Enable/disable scanning for connections to Botnet servers.
    disable    Do not scan for connections to botnet servers.
    block    Block connections to botnet servers.
    monitor    Log connections to botnet servers.
set label { string }    Label. size[63]
next
end
```


firewall internet-service

Introduction.

```
config firewall internet-service
  edit { id }
  # Show Internet Service application.
  set id { integer }   Internet Service ID. range[0-4294967295]
  set name { string }  Internet Service name. size[63]
  set reputation { integer } Reputation level of the Internet Service. range[0-4294967295]
  set icon-id { integer } Icon ID of Internet Service. range[0-4294967295]
  set offset { integer } Offset of Internet Service ID. range[0-4294967295]
  config entry
    edit { id }
    # Entries in the Internet Service database.
    set id { integer }   Entry ID. range[0-4294967295]
    set protocol { integer } Integer value for the protocol type as defined by IANA (0 - 255). range[0-255]
    set port { integer } Integer value for the TCP/IP port (0 - 65535). range[0-65535]
    set ip-range-number { integer } Total number of IP ranges. range[0-4294967295]
    set ip-number { integer } Total number of IP addresses. range[0-65535]
  next
next
end
```

firewall internet-service-custom

Introduction.

```

config firewall internet-service-custom
  edit { name }
  # Configure custom Internet Services.
  set name { string }   Internet Service name. size[63]
  set master-service-id { integer }   Internet Service ID in the Internet Service database. range[0-4294967295] - datasource(s): fire-
wall.internet-service.id
  set comment { string }   Comment. size[255]
  config entry
    edit { id }
    # Entries added to the Internet Service database and custom database.
    set id { integer }   Entry ID(1-255). range[0-255]
    set protocol { integer }   Integer value for the protocol type as defined by IANA (0 - 255). range[0-255]
    config port-range
      edit { id }
      # Port ranges in the custom entry.
      set id { integer }   Custom entry port range ID. range[0-4294967295]
      set start-port { integer }   Integer value for starting TCP/UDP/SCTP destination port in range (1 to 65535). range[1-65535]
      set end-port { integer }   Integer value for ending TCP/UDP/SCTP destination port in range (1 to 65535). range[1-65535]
    next
  config dst
    edit { name }
    # Destination address or address group name.
    set name { string }   Select the destination address or address group object from available options. size[64] - datasource
(s): firewall.address.name,firewall.addrgrp.name
    next
  next
  config disable-entry
    edit { id }
    # Disable entries in the Internet Service database.
    set id { integer }   Disable entry ID. range[0-4294967295]
    set protocol { integer }   Integer value for the protocol type as defined by IANA (0 - 255). range[0-255]
    set port { integer }   Integer value for the TCP/IP port (0 - 65535). range[0-65535]
    config ip-range
      edit { id }
      # IP ranges in the disable entry.

```

```
        set id { integer }    Disable entry range ID. range[0-4294967295]
        set start-ip { ipv4 address any }  Start IP address.
        set end-ip { ipv4 address any }    End IP address.
    next
next
next
end
```

firewall ipmacbinding setting

Introduction.

```
config firewall ipmacbinding setting
  set bindthroughfw { enable | disable }  Enable/disable use of IP/MAC binding to filter packets that would normally go through the firewall.
  set bindtofw { enable | disable }  Enable/disable use of IP/MAC binding to filter packets that would normally go to the firewall.
  set undefinedhost { allow | block }  Select action to take on packets with IP/MAC addresses not in the binding list (default = block).
    allow  Allow packets from MAC addresses not in the IP/MAC list.
    block  Block packets from MAC addresses not in the IP/MAC list.
end
```

firewall ipmacbinding table

Introduction.

```
config firewall ipmacbinding table
  edit { seq-num }
  # Configure IP to MAC address pairs in the IP/MAC binding table.
  set seq-num { integer }  Entry number. range[0-4294967295]
  set ip { ipv4 address }   IPv4 address portion of the pair (format: xxx.xxx.xxx.xxx).
  set mac { mac address }  MAC address portion of the pair (format: xx:xx:xx:xx:xx:xx in hexadecimal).
  set name { string }      Name of the pair (optional, default = no name). size[35]
  set status { enable | disable }  Enable/disable this IP-mac binding pair.
next
end
```

firewall {ippool | ippool6}

Introduction.

```

config firewall ippool
  edit { name }
  # Configure IPv4 IP pools.
  set name { string }   IP pool name. size[35]
  set type { overload | one-to-one | fixed-port-range | port-block-allocation }   IP pool type (overload, one-to-one, fixed port range, or port
block allocation).
  overload              IP addresses in the IP pool can be shared by clients.
  one-to-one           One to one mapping.
  fixed-port-range     Fixed port range.
  port-block-allocation Port block allocation.
  set startip { ipv4 address any }   First IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default:
0.0.0.0).
  set endip { ipv4 address any }   Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).
  set source-startip { ipv4 address any }   First IPv4 address (inclusive) in the range of the source addresses to be translated (format
xxx.xxx.xxx.xxx, Default: 0.0.0.0).
  set source-endip { ipv4 address any }   Final IPv4 address (inclusive) in the range of the source addresses to be translated (format
xxx.xxx.xxx.xxx, Default: 0.0.0.0).
  set block-size { integer }   Number of addresses in a block (64 to 4096, default = 128). range[64-4096]
  set num-blocks-per-user { integer }   Number of addresses blocks that can be used by a user (1 to 128, default = 8). range[1-128]
  set permit-any-host { disable | enable }   Enable/disable full cone NAT.
  set arp-reply { disable | enable }   Enable/disable replying to ARP requests when an IP Pool is added to a policy (default = enable).
  set arp-intf { string }   Select an interface from available options that will reply to ARP requests. (If blank, any is selected). size[15] -
datasource(s): system.interface.name
  set associated-interface { string }   Associated interface name. size[15] - datasource(s): system.interface.name
  set comments { string }   Comment. size[255]
  next
end

config firewall ippool6
  edit { name }
  # Configure IPv6 IP pools.
  set name { string }   IPv6 IP pool name. size[35]
  set startip { ipv6 address }   First IPv6 address (inclusive) in the range for the address pool (format

```

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, Default: :).  
    set endip { ipv6 address }    Final IPv6 address (inclusive) in the range for the address pool (format  
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, Default: :).  
    set comments { string }    Comment. size[255]  
next  
end
```

firewall ip-translation

Introduction.

```
config firewall ip-translation
  edit { transid }
    # Configure firewall IP-translation.
    set transid { integer } IP translation ID. range[0-4294967295]
    set type { Sctp } IP translation type (option: Sctp).
      Sctp Sctp
    set startip { ipv4 address any } First IPv4 address (inclusive) in the range of the addresses to be translated (format xxx.xxx.xxx.xxx,
default: 0.0.0.0).
    set endip { ipv4 address any } Final IPv4 address (inclusive) in the range of the addresses to be translated (format xxx.xxx.xxx.xxx,
default: 0.0.0.0).
    set map-startip { ipv4 address any } Address to be used as the starting point for translation in the range (format xxx.xxx.xxx.xxx,
default: 0.0.0.0).
    next
  end
```


firewall ipv6-eh-filter

Introduction.

```
config firewall ipv6-eh-filter
  set hop-opt { enable | disable }  Enable/disable blocking packets with the Hop-by-Hop Options header (default = disable).
  set dest-opt { enable | disable }  Enable/disable blocking packets with Destination Options headers (default = disable).
  set hdopt-type { integer }  Block specific Hop-by-Hop and/or Destination Option types (max. 7 types, each between 0 and 255, default = 0). range
[0-255]
  set routing { enable | disable }  Enable/disable blocking packets with Routing headers (default = enable).
  set routing-type { integer }  Block specific Routing header types (max. 7 types, each between 0 and 255, default = 0). range[0-255]
  set fragment { enable | disable }  Enable/disable blocking packets with the Fragment header (default = disable).
  set auth { enable | disable }  Enable/disable blocking packets with the Authentication header (default = disable).
  set no-next { enable | disable }  Enable/disable blocking packets with the No Next header (default = disable)
end
```

firewall ldb-monitor

Introduction.

```
config firewall ldb-monitor
  edit { name }
    # Configure server load balancing health monitors.
    set name { string } Monitor name. size[35]
    set type { ping | tcp | http } Select the Monitor type used by the health check monitor to check the health of the server (PING | TCP |
HTTP).
        ping PING health monitor.
        tcp TCP-connect health monitor.
        http HTTP-GET health monitor.
    set interval { integer } Time between health checks (5 - 65635 sec, default = 10). range[5-65535]
    set timeout { integer } 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). range[1-255]
    set retry { integer } Number health check attempts before the server is considered down (1 - 255, default = 3).. range[1-255]
    set port { integer } Service port used to perform the health check. If 0, health check monitor inherits port configured for the server (0 -
65635, default = 0). range[0-65535]
    set http-get { string } URL used to send a GET request to check the health of an HTTP server. size[255]
    set http-match { string } String to match the value expected in response to an HTTP-GET request. size[255]
    set http-max-redirects { integer } The maximum number of HTTP redirects to be allowed (0 - 5, default = 0). range[0-5]
  next
end
```

firewall {local-in-policy | local-in-policy6}

Introduction.

```

config firewall local-in-policy
  edit { policyid }
  # Configure user defined IPv4 local-in policies.
  set policyid { integer }  User defined local in policy ID. range[0-4294967295]
  set ha-mgmt-intf-only { enable | disable }  Enable/disable dedicating the HA management interface only for local-in policy.
  set intf { string }  Incoming interface name from available options. size[35] - datasource(s): system.zone.name,system.interface.name
  config srcaddr
    edit { name }
    # Source address object from available options.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  config dstaddr
    edit { name }
    # Destination address object from available options.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  set action { accept | deny }  Action performed on traffic matching the policy (default = deny).
    accept  Allow traffic matching this policy.
    deny    Deny or block traffic matching this policy.
  config service
    edit { name }
    # Service object from available options.
    set name { string }  Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
    next
  set schedule { string }  Schedule object from available options. size[35] - datasource(s): fire-
wall.schedule.onetime.name,firewall.schedule.recurring.name,firewall.schedule.group.name
  set status { enable | disable }  Enable/disable this local-in policy.
  next
end

config firewall local-in-policy6
  edit { policyid }
  # Configure user defined IPv6 local-in policies.

```

```
set policyid { integer } User defined local in policy ID. range[0-4294967295]
set intf { string } Incoming interface name from available options. size[35] - datasource(s): system.zone.name,system.interface.name
config srcaddr
  edit { name }
    # Source address object from available options.
    set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
config dstaddr
  edit { name }
    # Destination address object from available options.
    set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
set action { accept | deny } Action performed on traffic matching the policy (default = deny).
  accept Allow local-in traffic matching this policy.
  deny Deny or block local-in traffic matching this policy.
config service
  edit { name }
    # Service object from available options. Separate names with a space.
    set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
  set schedule { string } Schedule object from available options. size[35] - datasource(s): firewall.schedule.onetime.name,firewall.schedule.recurring.name,firewall.schedule.group.name
  set status { enable | disable } Enable/disable this local-in policy.
next
end
```

firewall {multicast-address | multicast-address6}

Introduction.

```

config firewall multicast-address
  edit { name }
  # Configure multicast addresses.
  set name { string } Multicast address name. size[63]
  set type { multicastrange | broadcastmask } Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.
    multicastrange Multicast range.
    broadcastmask Broadcast IP/mask.
  set subnet { ipv4 classnet any } Broadcast address and subnet.
  set start-ip { ipv4 address any } First IPv4 address (inclusive) in the range for the address.
  set end-ip { ipv4 address any } Final IPv4 address (inclusive) in the range for the address.
  set comment { string } Comment. size[255]
  set visibility { enable | disable } Enable/disable visibility of the multicast address on the GUI.
  set associated-interface { string } Interface associated with the address object. When setting up a policy, only addresses associated with this interface are available. size[35] - datasource(s): system.interface.name
  set color { integer } Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1). range[0-32]
  config tags
    edit { name }
    # Names of object-tags (as configured in config system object-tag) applied to address.
    set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
end

config firewall multicast-address6
  edit { name }
  # Configure IPv6 multicast address.
  set name { string } IPv6 multicast address name. size[63]
  set ip6 { ipv6 network } IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).
  set comment { string } Comment. size[255]
  set visibility { enable | disable } Enable/disable visibility of the IPv6 multicast address on the GUI.
  set color { integer } Color of icon on the GUI. range[0-32]
  config tags

```

```
edit { name }
# Applied object tags.
  set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
next
end
```

firewall {multicast-policy | multicast-policy6}

Introduction.

```

config firewall multicast-policy
  edit { id }
  # Configure multicast NAT policies.
  set id { integer } Policy ID. range[0-4294967294]
  set status { enable | disable } Enable/disable this policy.
  set logtraffic { enable | disable } Enable/disable logging traffic accepted by this policy.
  set srcintf { string } Source interface name. size[35] - datasource(s): system.interface.name
  set dstintf { string } Destination interface name. size[35] - datasource(s): system.interface.name
  config srcaddr
    edit { name }
    # Source address objects.
    set name { string } Source address objects. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstaddr
    edit { name }
    # Destination address objects.
    set name { string } Destination address objects. size[64] - datasource(s): firewall.multicast-address.name
  next
  set snat { enable | disable } Enable/disable substitution of the outgoing interface IP address for the original source IP address (called
source NAT or SNAT).
  set snat-ip { ipv4 address } IPv4 address to be used as the source address for NATed traffic.
  set dnat { ipv4 address any } IPv4 DNAT address used for multicast destination addresses.
  set action { accept | deny } Accept or deny traffic matching the policy.
    accept Accept traffic matching the policy.
    deny Deny or block traffic matching the policy.
  set protocol { integer } Integer value for the protocol type as defined by IANA (0 - 255, default = 0). range[0-255]
  set start-port { integer } Integer value for starting TCP/UDP/SCTP destination port in range (1 - 65535, default = 1). range[0-65535]
  set end-port { integer } Integer value for ending TCP/UDP/SCTP destination port in range (1 - 65535, default = 1). range[0-65535]
  set auto-asic-offload { enable | disable } Enable/disable offloading policy traffic for hardware acceleration.
  next
end

config firewall multicast-policy6

```

```
edit { id }
# Configure IPv6 multicast NAT policies.
  set id { integer } Policy ID. range[0-4294967294]
  set status { enable | disable } Enable/disable this policy.
  set logtraffic { enable | disable } Enable/disable logging traffic accepted by this policy.
  set srcintf { string } IPv6 source interface name. size[35] - datasource(s): system.interface.name
  set dstintf { string } IPv6 destination interface name. size[35] - datasource(s): system.interface.name
  config srcaddr
    edit { name }
    # IPv6 source address name.
    set name { string } Address name. size[79] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
    next
  config dstaddr
    edit { name }
    # IPv6 destination address name.
    set name { string } Address name. size[79] - datasource(s): firewall.multicast-address6.name
    next
  set action { accept | deny } Accept or deny traffic matching the policy.
    accept Accept.
    deny Deny.
  set protocol { integer } Integer value for the protocol type as defined by IANA (0 - 255, default = 0). range[0-255]
  set start-port { integer } Integer value for starting TCP/UDP/SCTP destination port in range (1 - 65535, default = 1). range[0-65535]
  set end-port { integer } Integer value for ending TCP/UDP/SCTP destination port in range (1 - 65535, default = 65535). range[0-65535]
  set auto-asic-offload { enable | disable } Enable/disable offloading policy traffic for hardware acceleration.
next
end
```


firewall {policy | policy6}

Used to change firewall policies or their individual configurations. In addition to editing an existing policy, policies can be added, deleted, moved or cloned. It is also possible to purge all of the policy content from the table that holds them.

- Use `config firewall policy` for IPv4 policies
- Use `config firewall policy6` for IPv6 policies

Firewall policies control all traffic passing through the FortiGate unit. Firewall policies are instructions used by the FortiGate unit to decide what to do with a connection request. The policy directs the firewall to allow the connection, deny the connection, require authentication before the connection is allowed, or apply IPSec processing. The commands `config firewall policy` and `config firewall policy6` enter the system into the correct context of the configuration file to make changes to firewall policies. From here, a specific policy is chosen to be acted upon.

```
config firewall policy
  edit { policyid }
  # Configure IPv4 policies.
  set policyid { integer } Policy ID. range[0-4294967294]
  set name { string } Policy name. size[35]
  set uuid { uuid } Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  config srcintf
    edit { name }
    # Incoming (ingress) interface.
    set name { string } Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
  config dstintf
    edit { name }
    # Outgoing (egress) interface.
    set name { string } Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
  config srcaddr
    edit { name }
    # Source address and address group names.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstaddr
    edit { name }
    # Destination address and address group names.
    set name { string } Address name. size[64] - datasource(s):
```

```
firewall.address.name, firewall.addrgrp.name, firewall.vip.name, firewall.vipgrp.name
    next
    set internet-service { enable | disable } Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.
    config internet-service-id
        edit { id }
        # Internet Service ID.
        set id { integer } Internet Service ID. range[0-4294967295] - datasource(s): firewall.internet-service.id
    next
    config internet-service-custom
        edit { name }
        # Custom Internet Service Name.
        set name { string } Custom Internet Service name. size[64] - datasource(s): firewall.internet-service-custom.name
    next
    set rtp-nat { disable | enable } Enable Real Time Protocol (RTP) NAT.
    config rtp-addr
        edit { name }
        # Address names if this is an RTP NAT policy.
        set name { string } Address name. size[64] - datasource(s): firewall.address.name, firewall.addrgrp.name
    next
    set learning-mode { enable | disable } Enable to allow everything, but log all of the meaningful data for security information gathering. A learning report will be generated.
    set action { accept | deny | ipsec } Policy action (allow/deny/ipsec).
        accept Allows session that match the firewall policy.
        deny Blocks sessions that match the firewall policy.
        ipsec Firewall policy becomes a policy-based IPsec VPN policy.
    set send-deny-packet { disable | enable } Enable to send a reply when a session is denied or blocked by a firewall policy.
    set firewall-session-dirty { check-all | check-new } How to handle sessions if the configuration of this firewall policy changes.
        check-all Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.
        check-new Continue to allow sessions already accepted by this policy.
    set status { enable | disable } Enable or disable this policy.
    set schedule { string } Schedule name. size[35] - datasource(s): firewall.schedule.onetime.name, firewall.schedule.recurring.name, firewall.schedule.group.name
    set schedule-timeout { enable | disable } Enable to force current sessions to end when the schedule object times out. Disable allows them to end from inactivity.
    config service
        edit { name }
        # Service and service group names.
        set name { string } Service and service group names. size[64] - datasource(s): firewall.service.custom.name, firewall.service.group.name
    next
    set dscp-match { enable | disable } Enable DSCP check.
    set dscp-negate { enable | disable } Enable negated DSCP match.
```

```

set dscp-value { string } DSCP value.
set tcp-session-without-syn { all | data-only | disable } Enable/disable creation of TCP session without SYN flag.
    all Enable TCP session without SYN.
    data-only Enable TCP session data only.
    disable Disable TCP session without SYN.
set utm-status { enable | disable } Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.
set profile-type { single | group } Determine whether the firewall policy allows security profile groups or single profiles only.
    single Do not allow security profile groups.
    group Allow security profile groups.
set profile-group { string } Name of profile group. size[35] - datasource(s): firewall.profile-group.name
set av-profile { string } Name of an existing Antivirus profile. size[35] - datasource(s): antivirus.profile.name
set webfilter-profile { string } Name of an existing Web filter profile. size[35] - datasource(s): webfilter.profile.name
set dnsfilter-profile { string } Name of an existing DNS filter profile. size[35] - datasource(s): dnsfilter.profile.name
set spamfilter-profile { string } Name of an existing Spam filter profile. size[35] - datasource(s): spamfilter.profile.name
set dlp-sensor { string } Name of an existing DLP sensor. size[35] - datasource(s): dlp.sensor.name
set ips-sensor { string } Name of an existing IPS sensor. size[35] - datasource(s): ips.sensor.name
set application-list { string } Name of an existing Application list. size[35] - datasource(s): application.list.name
set voip-profile { string } Name of an existing VoIP profile. size[35] - datasource(s): voip.profile.name
set icap-profile { string } Name of an existing ICAP profile. size[35] - datasource(s): icap.profile.name
set waf-profile { string } Name of an existing Web application firewall profile. size[35] - datasource(s): waf.profile.name
set profile-protocol-options { string } Name of an existing Protocol options profile. size[35] - datasource(s): firewall.profile-protocol-
options.name
set ssl-ssh-profile { string } Name of an existing SSL SSH profile. size[35] - datasource(s): firewall.ssl-ssh-profile.name
set logtraffic { all | utm | disable } Enable or disable logging. Log all sessions or security profile sessions.
    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.
set logtraffic-start { enable | disable } Record logs when a session starts and ends.
set capture-packet { enable | disable } Enable/disable capture packets.
set auto-asic-offload { enable | disable } Enable/disable offloading security profile processing to CP processors.
set np-accelation { enable | disable } Enable/disable UTM Network Processor acceleration.
set wanopt { enable | disable } Enable/disable WAN optimization.
set wanopt-detection { active | passive | off } WAN optimization auto-detection mode.
    active Active WAN optimization peer auto-detection.
    passive Passive WAN optimization peer auto-detection.
    off Turn off WAN optimization peer auto-detection.
set wanopt-passive-opt { default | transparent | non-transparent } WAN optimization passive mode options. This option decides what IP
address will be used to connect server.
    default Allow client side WAN opt peer to decide.
    transparent Use address of client to connect to server.
    non-transparent Use local FortiGate address to connect to server.
set wanopt-profile { string } WAN optimization profile. size[35] - datasource(s): wanopt.profile.name
set wanopt-peer { string } WAN optimization peer. size[35] - datasource(s): wanopt.peer.peer-host-id

```

```
set webcache { enable | disable } Enable/disable web cache.
set webcache-https { disable | enable } Enable/disable web cache for HTTPS.
set traffic-shaper { string } Traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set traffic-shaper-reverse { string } Reverse traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set per-ip-shaper { string } Per-IP traffic shaper. size[35] - datasource(s): firewall.shaper.per-ip-shaper.name
config application
  edit { id }
  # Application ID list.
  set id { integer } Application IDs. range[0-4294967295]
  next
config app-category
  edit { id }
  # Application category ID list.
  set id { integer } Category IDs. range[0-4294967295]
  next
config url-category
  edit { id }
  # URL category ID list.
  set id { integer } URL category ID. range[0-4294967295]
  next
set nat { enable | disable } Enable/disable source NAT.
set permit-any-host { enable | disable } Accept UDP packets from any host.
set permit-stun-host { enable | disable } Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.
set fixedport { enable | disable } Enable to prevent source NAT from changing a session's source port.
set ippool { enable | disable } Enable to use IP Pools for source NAT.
config poolname
  edit { name }
  # IP Pool names.
  set name { string } IP pool name. size[64] - datasource(s): firewall.ippool.name
  next
set session-ttl { integer } Session TTL in seconds for sessions accepted by this policy. 0 means use the system default session TTL. range
[300-604800]
set vlan-cos-fwd { integer } VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest. range[0-7]
set vlan-cos-rev { integer } VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest.. range[0-7]
set inbound { enable | disable } Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.
set outbound { enable | disable } Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.
set natinbound { enable | disable } Policy-based IPsec VPN: apply destination NAT to inbound traffic.
set natoutbound { enable | disable } Policy-based IPsec VPN: apply source NAT to outbound traffic.
set wccp { enable | disable } Enable/disable forwarding traffic matching this policy to a configured WCCP server.
set ntlm { enable | disable } Enable/disable NTLM authentication.
set ntlm-guest { enable | disable } Enable/disable NTLM guest user access.
config ntlm-enabled-browsers
  edit { user-agent-string }
```

```

# HTTP-User-Agent value of supported browsers.
    set user-agent-string { string } User agent string. size[64]
    next
set fsso { enable | disable } Enable/disable Fortinet Single Sign-On.
set wssso { enable | disable } Enable/disable WiFi Single Sign On (WSSO).
set rssso { enable | disable } Enable/disable RADIUS single sign-on (RSSO).
set fsso-agent-for-ntlm { string } FSSO agent to use for NTLM authentication. size[35] - datasource(s): user.fsso.name
config groups
    edit { name }
    # Names of user groups that can authenticate with this policy.
    set name { string } Group name. size[64] - datasource(s): user.group.name
    next
config users
    edit { name }
    # Names of individual users that can authenticate with this policy.
    set name { string } Names of individual users that can authenticate with this policy. size[64] - datasource(s): user.local.name
    next
config devices
    edit { name }
    # Names of devices or device groups that can be matched by the policy.
    set name { string } Device or group name. size[35] - datasource(s): user.device.alias,user.device-group.name,user.device-cat-
egory.name
    next
    set auth-path { enable | disable } Enable/disable authentication-based routing.
    set disclaimer { enable | disable } Enable/disable user authentication disclaimer.
    set vpntunnel { string } Policy-based IPsec VPN: name of the IPsec VPN Phase 1. size[35] - datasource(s): vpn.ipsec.phase1.-
name,vpn.ipsec.manualkey.name
    set natip { ipv4 classnet } Policy-based IPsec VPN: source NAT IP address for outgoing traffic.
    set match-vip { enable | disable } Enable to match packets that have had their destination addresses changed by a VIP.
    set diffserv-forward { enable | disable } Enable to change packet's DiffServ values to the specified diffservcode-forward value.
    set diffserv-reverse { enable | disable } Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev
value.
    set diffservcode-forward { string } Change packet's DiffServ to this value.
    set diffservcode-rev { string } Change packet's reverse (reply) DiffServ to this value.
    set tcp-mss-sender { integer } Sender TCP maximum segment size (MSS). range[0-65535]
    set tcp-mss-receiver { integer } Receiver TCP maximum segment size (MSS). range[0-65535]
    set comments { string } Comment. size[1023]
    set label { string } Label for the policy that appears when the GUI is in Section View mode. size[63]
    set global-label { string } Label for the policy that appears when the GUI is in Global View mode. size[63]
    set auth-cert { string } HTTPS server certificate for policy authentication. size[35] - datasource(s): vpn.certificate.local.name
    set auth-redirect-addr { string } HTTP-to-HTTPS redirect address for firewall authentication. size[63]
    set redirect-url { string } URL users are directed to after seeing and accepting the disclaimer or authenticating. size[255]
    set identity-based-route { string } Name of identity-based routing rule. size[35] - datasource(s): firewall.identity-based-route.name

```

```
set block-notification { enable | disable } Enable/disable block notification.
config custom-log-fields
  edit { field-id }
  # Log field index numbers to append custom log fields to log messages for this policy.
  set field-id { string } Custom log field. size[35] - datasource(s): log.custom-field.id
  next
config tags
  edit { name }
  # Names of object-tags applied to this policy.
  set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
set replacemsg-override-group { string } Override the default replacement message group for this policy. size[35] - datasource(s): system.replacemsg-group.name
set srcaddr-negate { enable | disable } When enabled srcaddr specifies what the source address must NOT be.
set dstaddr-negate { enable | disable } When enabled dstaddr specifies what the destination address must NOT be.
set service-negate { enable | disable } When enabled service specifies what the service must NOT be.
set internet-service-negate { enable | disable } When enabled internet-service specifies what the service must NOT be.
set timeout-send-rst { enable | disable } Enable/disable sending RST packets when TCP sessions expire.
set captive-portal-exempt { enable | disable } Enable to exempt some users from the captive portal.
set ssl-mirror { enable | disable } Enable to copy decrypted SSL traffic to a FortiGate interface (called SSL mirroring).
config ssl-mirror-intf
  edit { name }
  # SSL mirror interface name.
  set name { string } Mirror Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
set scan-botnet-connections { disable | block | monitor } Block or monitor connections to Botnet servers or disable Botnet scanning.
  disable Do not scan connections to botnet servers.
  block Block connections to botnet servers.
  monitor Log connections to botnet servers.
set dsri { enable | disable } Enable DSRI to ignore HTTP server responses.
set radius-mac-auth-bypass { enable | disable } Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.
set delay-tcp-npu-session { enable | disable } Enable TCP NPU session delay to guarantee packet order of 3-way handshake.
  next
end

config firewall policy6
  edit { policyid }
  # Configure IPv6 policies.
  set policyid { integer } Policy ID. range[0-4294967294]
  set name { string } Policy name. size[35]
  set uuid { uuid } Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
```

```

config srcintf
  edit { name }
  # Incoming (ingress) interface.
  set name { string }  Interface name. size[64] - datasource(s): system.zone.name,system.interface.name
  next
config dstintf
  edit { name }
  # Outgoing (egress) interface.
  set name { string }  Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
config srcaddr
  edit { name }
  # Source address and address group names.
  set name { string }  Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
config dstaddr
  edit { name }
  # Destination address and address group names.
  set name { string }  Address name. size[64] - datasource(s): fire-
wall.address6.name,firewall.addrgrp6.name,firewall.vip6.name,firewall.vipgrp6.name
  next
set action { accept | deny | ipsec }  Policy action (allow/deny/ipsec).
  accept  Allows session that match the firewall policy.
  deny    Blocks sessions that match the firewall policy.
  ipsec   Firewall policy becomes a policy-based IPsec VPN policy.
set firewall-session-dirty { check-all | check-new }  How to handle sessions if the configuration of this firewall policy changes.
  check-all  Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.
  check-new  Continue to allow sessions already accepted by this policy.
set status { enable | disable }  Enable or disable this policy.
set vlan-cos-fwd { integer }  VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest range[0-7]
set vlan-cos-rev { integer }  VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest range[0-7]
set schedule { string }  Schedule name. size[35] - datasource(s): fire-
wall.schedule.onetime.name,firewall.schedule.recurring.name,firewall.schedule.group.name
config service
  edit { name }
  # Service and service group names.
  set name { string }  Address name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
set dscp-match { enable | disable }  Enable DSCP check.
set dscp-negate { enable | disable }  Enable negated DSCP match.
set dscp-value { string }  DSCP value.
set tcp-session-without-syn { all | data-only | disable }  Enable/disable creation of TCP session without SYN flag.
  all  Enable TCP session without SYN.

```

```

    data-only Enable TCP session data only.
    disable Disable TCP session without SYN.
set utm-status { enable | disable } Enable AV/web/ips protection profile.
set profile-type { single | group } Determine whether the firewall policy allows security profile groups or single profiles only.
    single Do not allow security profile groups.
    group Allow security profile groups.
set profile-group { string } Name of profile group. size[35] - datasource(s): firewall.profile-group.name
set av-profile { string } Name of an existing Antivirus profile. size[35] - datasource(s): antivirus.profile.name
set webfilter-profile { string } Name of an existing Web filter profile. size[35] - datasource(s): webfilter.profile.name
set spamfilter-profile { string } Name of an existing Spam filter profile. size[35] - datasource(s): spamfilter.profile.name
set dlp-sensor { string } Name of an existing DLP sensor. size[35] - datasource(s): dlp.sensor.name
set ips-sensor { string } Name of an existing IPS sensor. size[35] - datasource(s): ips.sensor.name
set application-list { string } Name of an existing Application list. size[35] - datasource(s): application.list.name
set voip-profile { string } Name of an existing VoIP profile. size[35] - datasource(s): voip.profile.name
set icap-profile { string } Name of an existing ICAP profile. size[35] - datasource(s): icap.profile.name
set profile-protocol-options { string } Name of an existing Protocol options profile. size[35] - datasource(s): firewall.profile-protocol-
options.name
set ssl-ssh-profile { string } Name of an existing SSL SSH profile. size[35] - datasource(s): firewall.ssl-ssh-profile.name
set logtraffic { all | utm | disable } Enable or disable logging. Log all sessions or security profile sessions.
    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.
set logtraffic-start { enable | disable } Record logs when a session starts and ends.
set auto-asic-offload { enable | disable } Enable/disable policy traffic ASIC offloading.
set np-accelation { enable | disable } Enable/disable UTM Network Processor acceleration.
set traffic-shaper { string } Reverse traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set traffic-shaper-reverse { string } Reverse traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set per-ip-shaper { string } Per-IP traffic shaper. size[35] - datasource(s): firewall.shaper.per-ip-shaper.name
config application
    edit { id }
        # Application ID list.
        set id { integer } Application IDs. range[0-4294967295]
    next
config app-category
    edit { id }
        # Application category ID list.
        set id { integer } Category IDs. range[0-4294967295]
    next
config url-category
    edit { id }
        # URL category ID list.
        set id { integer } URL category ID. range[0-4294967295]
    next

```



```

set nat { enable | disable } Enable/disable source NAT.
set fixedport { enable | disable } Enable to prevent source NAT from changing a session's source port.
set ippool { enable | disable } Enable to use IP Pools for source NAT.
config poolname
  edit { name }
    # IP Pool names.
    set name { string } IP pool name. size[64] - datasource(s): firewall.ippool6.name
  next
set session-ttl { integer } Session TTL in seconds for sessions accepted by this policy. 0 means use the system default session TTL. range
[300-604800]
set inbound { enable | disable } Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.
set outbound { enable | disable } Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.
set natinbound { enable | disable } Policy-based IPsec VPN: apply destination NAT to inbound traffic.
set natoutbound { enable | disable } Policy-based IPsec VPN: apply source NAT to outbound traffic.
set send-deny-packet { enable | disable } Enable/disable return of deny-packet.
set vpngroup { string } Policy-based IPsec VPN: name of the IPsec VPN Phase 1. size[35] - datasource(s): vpn.ipsec.phasel.-
name,vpn.ipsec.manualkey.name
set diffserv-forward { enable | disable } Enable to change packet's DiffServ values to the specified diffservcode-forward value.
set diffserv-reverse { enable | disable } Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev
value.
set diffservcode-forward { string } Change packet's DiffServ to this value.
set diffservcode-rev { string } Change packet's reverse (reply) DiffServ to this value.
set tcp-mss-sender { integer } Sender TCP maximum segment size (MSS). range[0-65535]
set tcp-mss-receiver { integer } Receiver TCP maximum segment size (MSS). range[0-65535]
set comments { string } Comment. size[1023]
set label { string } Label for the policy that appears when the GUI is in Section View mode. size[63]
set global-label { string } Label for the policy that appears when the GUI is in Global View mode. size[63]
set rso { enable | disable } Enable/disable RADIUS single sign-on (RSSO).
config custom-log-fields
  edit { field-id }
    # Log field index numbers to append custom log fields to log messages for this policy.
    set field-id { string } Custom log field. size[35] - datasource(s): log.custom-field.id
  next
config tags
  edit { name }
    # Names of object-tags applied to this policy.
    set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
set replacemsg-override-group { string } Override the default replacement message group for this policy. size[35] - datasource(s): sys-
tem.replacemsg-group.name
set srcaddr-negate { enable | disable } When enabled srcaddr specifies what the source address must NOT be.
set dstaddr-negate { enable | disable } When enabled dstaddr specifies what the destination address must NOT be.
set service-negate { enable | disable } When enabled service specifies what the service must NOT be.

```

```

config groups
  edit { name }
  # Names of user groups that can authenticate with this policy.
  set name { string }  Group name. size[64] - datasource(s): user.group.name
  next
config users
  edit { name }
  # Names of individual users that can authenticate with this policy.
  set name { string }  Names of individual users that can authenticate with this policy. size[64] - datasource(s): user.local.name
  next
config devices
  edit { name }
  # Names of devices or device groups that can be matched by the policy.
  set name { string }  Device or group name. size[35] - datasource(s): user.device.alias,user.device-group.name,user.device-cat-
egory.name
  next
set timeout-send-rst { enable | disable }  Enable/disable sending RST packets when TCP sessions expire.
set ssl-mirror { enable | disable }  Enable to copy decrypted SSL traffic to a FortiGate interface (called SSL mirroring).
config ssl-mirror-intf
  edit { name }
  # SSL mirror interface name.
  set name { string }  Interface name. size[64] - datasource(s): system.zone.name,system.interface.name
  next
set dsri { enable | disable }  Enable DSRI to ignore HTTP server responses.
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

Managing policy objects

The configuration of specific policy options or settings is the most common activity when using the firewall policy command but some commands affect the policy objects as a whole.

edit

Used to select which individual policy to configure or edit values.

Syntax:

```
edit <policyid>
```

- Choosing 0 as the <policyid> will add a new policy using the next available number as the <policyid>. While first editing the policy the context at the command prompt will indicate that the <policyid> is 0 but subsequent editing will require going to the new <policyid>.

delete

Used to delete an existing firewall policy

Syntax:

```
delete <policyid>
```

- The <policyid> can be an integer value between 0 and 4294967294

purge

Used delete all of the existing firewall policies. It deletes all of the values within the table that holds the information about firewall policies within the VDOM.

Syntax:

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

move

Used to move the position of a policy, relative to another policy, in the sequence order of how policies are applied.

Syntax:

```
move <policyid> {after | before} <policyid>
```

clone

Used to copy all of the attributes of an existing policy to another policy.

Syntax:

```
clone <policyid> to <policyid>
```

Options and settings within a policy**name**

A unique name given to the policy. By default, this is a required field but the requirement can be disabled.

Syntax:

```
set name <string>
```

Examples:

```
config firewall policy
  edit 0
    set name example
  or..
  set name "example policy name"
end
```

uuid

Each policy has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited.

Syntax:

```
set uuid <uuid_value>
```

Default value: autogenerated

Example:

```
config firewall policy
  edit 0
```

```
        set uuid a3c9ccb8-a84a-51e6-d72c-6a5189cadb83
    end
```

srcintf

Sets the source interface of the traffic that the policy will manage. The value is a <string> that should be the name of one of the existing interfaces configured on the device. Separate multiple interfaces with a space.

Syntax:

```
{set|append} srcintf <name_of_interface> [<name_of_interface> ...]
```

Example:

```
config firewall policy
    edit 0
    set srcintf port1
    or ...
    set srcintf port2 port3
    or ...
    append srcintf port4
end
```

dstintf

Sets the destination interface of the traffic that the policy will manage. The value is a <string> that should be the name of one of the existing interfaces configured on the device. Separate multiple interfaces with a space.

Syntax:

```
{set|append} dstintf <name_of_interface> [<name_of_interface> ...]
```

Example:

```
config firewall policy
    edit 0
    set dstintf port11
    or ...
```

```
    set dstintf port12 port13
    or ...
    append dstintf port14
end
```

srcaddr

Sets the source address object(s), whose traffic will be managed by this policy. More than once object can be assigned to this option. Separate multiple addresses with a space.

Syntax:

```
{set|append} srcaddr <address_object> [<address_object> ...]
```

Examples:

```
config firewall policy
  edit 0
  set srcaddr example_address1
  or ...
  set srcaddress "example address2" "example_address3"
  or ...
  append srcaddr example_address4
end
```

dstaddr

Sets the destination address object(s), whose traffic will be managed by this policy. More than once object can be assigned to this option. Separate multiple addresses with a space.

Syntax:

```
{set|append} dstaddr <address_object> [<address_object> ...]
```

Examples:

```
config firewall policy
  edit 0
```

```
    set dstaddr example_address1
  or ...
  set dstaddr "example_address2" "example_address3"
  or ...
  append dstaddr example_address4
end
```

rtp-nat

Enables or disables the application of source NAT to RTP packets received by the firewall policy. This field is used for redundant SIP configurations. If `rtp-nat` is enabled you must add one or more firewall addresses to the `rtp-addr` field.

Syntax:

```
set rtp-nat {enable|disable}
```

Default value: `disable`

rtp-addr

Used to enter one or more RTP firewall addresses for the policy. This field is only available when `rtp-nat` is enabled. Separate multiple addresses with a space.

Syntax:

```
{set|append} rtp-addr <address_object> [<address_object> ...]
```

Examples:

```
config firewall policy
  edit 0
  set rtp-addr example_address1
  or ...
  set rtp-addr "example_address 2" "example_address3"
  or ...
  append example_address4
end
```

learning-mode

Enables or disables a specialized action option that monitors and logs traffic based on hard coded security profiles. See [Make it a policy to learn before configuring policies](#). Enabling `learning-mode` will make the `action` setting unavailable.

Syntax:

```
set learning-mode {enable|disable}
```

Default value: `disable`

action

Sets the action that the FortiGate unit will perform on traffic matching this firewall policy.

- `accept` — Allow packets that match the firewall policy. Optionally, also enable `nat` to make this a NAT policy (NAT/Route mode only).
- `deny` — Deny packets that match the firewall policy.
- `ipsec` — Allow and apply IPsec VPN. You must specify the `vpntunnel` attribute. You may also enable or disable the `inbound`, `outbound`, `natoutbound`, and `natinbound` attributes and/or specify a `natip` value.

Limitations:

- If `learning-mode` is enabled the `action` setting will not be available
- For IPv6 policies, only `accept` and `deny` options are available.

Syntax:

```
set action [accept|deny|ipsec]
```

Default value: `deny`

Examples:

```
config firewall policy
  edit 0
    set action accept
end
```


send-deny-packet

Enables or disables the ability to send a packet in reply to denied TCP, UDP or ICMP traffic. When deny-tcp-with-icmp is enabled in system settings, a Communication Prohibited ICMP packet is sent. Otherwise, denied TCP traffic is sent a TCP reset.

Syntax:

```
set send-deny-packet {enable|disable}
```

Default value: disable

firewall-session-dirty

Used to determine whether changes to a firewall policy affect all sessions or just new ones.

- `check-all` — flushes all current sessions in order to re-evaluate them
- `check-new` — keeps existing sessions and applies policy change only to new sessions

This field is available if `firewall-session-dirty` in `config system settings` is set to `check-policy-option`.

Syntax:

```
set firewall-session-dirty [check-all|check-new]
```

Default value: check-all

Examples:

```
config firewall policy
    edit 0
        set firewall-session-dirty check-new
    end
```

status

Enables or disables a policy.

Syntax:

```
set status {enable|disable}
```

Default value: enable

schedule

Sets the schedule used by the policy. The variable is the name of the existing one-time or reoccurring schedule, or schedule group.

Syntax:

```
set schedule <schedule_object>
```

Examples:

```
config firewall policy
    edit 0
        set schedule work_week
    end
```

schedule-timeout

When enabled, sessions are forced to end when the schedule's end time is reached. If disabled, sessions can go past the schedule's end time, but no new sessions can start.

Syntax:

```
set schedule-timeout {enable|disable}
```

Default value: disable

service

Used to set the services matched by the policy. The variable can be one or more services or service groups. Separate multiple services with a space.

Syntax:

```
{set|append} service <service_object> [<service_object> ...]
```

Examples:

```
config firewall policy
  edit 0
  set service http
  or ...
  set service http "Email Access"
  or ...
  append service ftp
end
```

utm-status

Enables or disables adding security profiles on the firewall policy. If enabled, at least one profile must be added to the policy. This setting is not available until the source and destination parameters of the policy have been configured.

Syntax:

```
set utm-status {enable|disable}
```

Default value: disable

profile-type

Sets whether or not to use individual UTM profiles or a UTM profile group to the firewall policy.

Syntax:

```
set profile-type {single | group}
```

Default value: single

Examples:

```
config firewall policy
  edit 0
```

```
        set profile-type group
    end
```

profile-group

Determines the name of a UTM profile group in the firewall policy. This option is available if `profile-type` is set to `group`.

Syntax:

```
set profile-group <string>
```

Examples:

```
config firewall policy
    edit 0
        set profile-group example_profile_group
    end
```

av-profile

Sets the name of the antivirus profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set av-profile <string>
```

Examples:

```
config firewall policy
    edit 0
        set av-profile default_av_profile
    end
```

webfilter-profile

Sets the name of the webfilter profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set webfilter-profile <string>
```

Example:

```
config firewall policy
    edit 0
        set webfilter-profile "example web profile"
    end
```

dnsfilter-profile

Sets the name of the DNS filter profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set dnsfilter-profile <string>
```

Examples:

```
config firewall policy
    edit 0
        set dnsfilter-profile dns_for_developers
    end
```

spamfilter-profile

Sets the name of the spam filter profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set spamfilter-profile <string>
```

Examples:

```
config firewall policy
    edit 0
```

```
        set spamfilter-profile spam-filter1
    end
```

dlp-sensor

Sets the name of the DLP sensor profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set dlp-sensor <string>
```

Examples:

```
config firewall policy
    edit 0
        set dlp-sensor dlp-classified
    end
```

ips-sensor

Sets the name of the IPS profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set ips-sensor <string>
```

Examples:

```
config firewall policy
    edit 0
        set ips-sensor production_ips
    end
```

application-list

Sets the name of the pre-packaged list of applications associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set application-list <string>
```

Examples:

```
config firewall policy
    edit 0
        set application-list allowed-apps
    end
```

casi-profile

Sets the name of the CASI profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set casi-profile <string>
```

Examples:

```
config firewall policy
    edit 0
        set casi-profile casi-default
    end
```

voip-profile

Sets the name of the VoIP profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set voip-profile <string>
```

Examples:

```
config firewall policy
    edit 0
```

```
        set voip-profile voip-example
    end
```

icap-profile

Sets the name of the ICAP profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set icap-profile <string>
```

Examples:

```
config firewall policy
    edit 0
        set icap-profile icap-test
    end
```

waf-profile

Sets the name of the WAF profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set waf-profile <string>
```

Examples:

```
config firewall policy
    edit 0
        set waf-profile waf-profile1
    end
```

profile-protocol-options

Sets the name of the protocol options profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set profile-protocol-options <string>
```

Examples:

```
config firewall policy
    edit 0
        set profile-protocol-options company_default
    end
```

ssl-ssh-profile

Sets the name of the SSL/SSH profile associated with the firewall policy. This field is available only if `utm-status` is enabled.

Syntax:

```
set ssl-ssh-profile <string>
```

Examples:

```
config firewall policy
    edit 0
        set ssl-ssh-profile default-profile
    end
```

logtraffic

Used to set how traffic logs are recorded for this policy.

- `all` - record logs for all traffic accepted by this policy
- `utm log traffic` traffic that has a security profile applied to it
- `disable` - disable logging for this policy

Syntax:

```
set logtraffic {all | utm | disable}
```

Default value: utm

Example:

```
config firewall policy
    edit 0
        set logtraffic utm
    end
```

logtraffic-start

Enables or disables the ability to log session starts and stops.

Syntax:

```
set logtraffic-start {enable|disable}
```

Default value: disable

capture-packet

Enables or disables the packet capture feature. This is available if the `logtraffic` setting is `all` or `utm`.

Default value: disable

Syntax:

```
set capture-packet {enable|disable}
```

auto-asic-offload

Enables or disables offloading policy traffic to CP processors.

Syntax:

```
set auto-asic-offload {enable|disable}
```

Default value: disable

wanopt

Enables or disables the use the the WAN optimization feature on this policy. This feature is only available if the `action` setting is `accept`.

Syntax:

```
set wanopt {enable|disable}
```

Default value: `disable`

wanopt-detection

Used to select the wanopt peer auto-detection mode.

Syntax:

```
set wanopt-detection {active | passive | off}
```

Default value: `off`

Example:

```
config firewall policy
  edit 0
    set wanopt-detection active
end
```

wanopt-passive-opt

Used to set passive WAN Optimization policy address translation behavior.

- `default` - Use the transparent setting in the WAN Optimization profile added to the active policy (client-side configuration).
- `transparent` - Impose transparent mode (override the active policy transparent mode setting). Packets exiting the FortiGate keep their original source addresses.
- `non-transparent` - Impose non-transparent mode (override the active policy transparent mode setting). Packets exiting the FortiGate have their source address changed to the address of the server-side FortiGate unit interface that sends the packets to the servers.

Syntax:

```
set wanopt-passive-opt {default | transparent | non-transparent}
```

Default value: default

Example:

```
config firewall policy
    edit 0
        set wanopt-passive-opt transparent
end
```

wanopt-profile

Sets the name of the WAN optimization profile associated with the firewall policy.

Syntax:

```
set wanopt-profile <string>
```

Example:

```
config firewall policy
    edit 0
        set wanopt-profile "Company default WANopt"
end
```

wanopt-peer

Used to set the WAN optimization peer.

Syntax:

```
set wanopt-peer <string>
```

webcache

Enables or disables the WAN optimization web caching for HTTP traffic accepted by the firewall policy. This option is available only on FortiGate units that support WAN Optimization and web caching.

Syntax:

```
set webcache {enable|disable}
```

Default value: disable

webcache-https

Sets the level of webcaching for HTTPS traffic.

- `disable` — no caching of HTTPS traffic
- `enable` — caching of HTTPS traffic

This field is available only if `webcache` is enabled. This field is not available if `srcintf` is `ftp-proxy` or `wanopt`.

Syntax:

```
set webcache-https {disable| enable}
```

Default value: disable

Example:

```
config firewall policy
  edit 0
    set webcache enable
    set webcache-https enable
end
```

traffic-shaper

Select a traffic shaper for the policy. A traffic shaper controls the bandwidth available to, and sets the priority of the traffic processed by, the policy.

Syntax:

```
set traffic-shaper <string>
```

traffic-shaper-reverse

Select a reverse traffic shaper. For example, if the traffic direction that a policy controls is from port1 to port2, select this option will also apply the policy shaping configuration to traffic from port2 to port1.

Syntax:

```
set traffic-shaper-reverse <string>
```

per-ip-shaper

Enter the name of the per-IP traffic shaper to associate with this policy. For information about per-IP traffic shapers, see `firewall shaper per-ip-shaper`.

Syntax:

```
set per-ip-shaper <string>
```

nat

Enables or disables the use of Network Address Translation (NAT)

Syntax:

```
set nat {enable|disable}
```

Default value: disable

permit-any-host

Enables or disables the ability to accept UDP packets from any host. This can help support the FaceTime application on NAT'd iPhones.

Syntax:

```
set permit-any-host {enable|disable}
```

Default value: `disable`

permit-stun-host

Enables or disables the ability to accept UDP packets from any Session Traversal Utilities for NAT (STUN) host. This can help support the FaceTime application on NAT'd iPhones.

Syntax:

```
set permit-stun-host {enable|disable}
```

Default value: `disable`

fixedport

Enables or disables the ability to preserve packets' source port number, which may otherwise be changed by a NAT policy. Some applications do not function correctly if the source port number is changed, and may require this option. If `fixedport` is `enable`, you should usually also enable IP pools; if you do not configure an IP pool for the policy, only one connection can occur at a time for this port.

Syntax:

```
set fixedport {enable|disable}
```

Default value: `disable`

ippool

Enables or disables the use of ippools for NAT. When the `action` is set to `accept` and NAT is enabled, the `ippool` function allows a NAT policy to translate the source address to an address randomly selected from the first IP pool added to the destination interface of the policy.

Syntax:

```
set ippool {enable|disable}
```

Default value: `disable`

poolname

The name of the IP pool to be used for NAT. To use this option requires that `ippool` be enabled. Separate multiple addresses with a space.

Syntax:

```
{set|append} poolname <ippool> [<ippool> ...]
```

Example:

```
config firewall policy
  edit 0
  set poolname testpool1
  or ...
  append poolname "testpool 1" "testpool2"
  or ...
  clear poolname
end
```

session-ttl

Used to set the timeout value in the policy to override the global timeout setting defined by using `config system session-ttl`. When it is on default value, it will not take effect. Value is in seconds.

Syntax:

```
set session-ttl <integer>
```

Default value: 0

Example:

```
config firewall policy
  edit 0
  set session-ttl 3600
end
```

vlan-cos-fwd

Used to set the VLAN forward direction user priority, CoS. Range 0 (lowest) to 7 (highest), 255 for passthrough.

Syntax:

```
set vlan-cos-fwd <integer>
```

Default value: 255

Example:

```
config firewall policy
    edit 0
        set vlan-cos-fwd 7
end
```

vlan-cos-rev

Used to set the VLAN reverse direction user priority, CoS. Range 0 (lowest) to 7 (highest), 255 for passthrough.

Syntax:

```
set vlan-cos-rev <integer>
```

Default value: 255

Example:

```
config firewall policy
    edit 0
        set vlan-cos-rev 3
end
```

inbound

When `action` is set to `ipsec`, this setting enables or disables traffic from computers on the remote private network to initiate an IPsec VPN tunnel.

Syntax:

```
set inbound {enable | disable}
```

Default value: disable

outbound

When `action` is set to `ipsec`, this setting enables or disables traffic from computers on the local private network to initiate an IPsec VPN tunnel.

Syntax:

```
set outbound {enable | disable}
```

Default value: `disable`

natinbound

Enables or disables the function of translating the source addresses IP packets emerging from an IPsec tunnel into the IP address of the FortiGate unit's network interface to the local private network. This option appears only if `action` is `ipsec`.

Syntax:

```
set natinbound {enable | disable}
```

Default value: `disable`

natoutbound

Enables or disables the function of translating the source addresses of outbound encrypted packets into the IP address of the FortiGate unit's outbound interface. Enable this attribute in combination with the `natip` attribute to change the source addresses of IP packets before they go into the tunnel. This option appears only if attribute to change the source addresses of IP packets before they go into the tunnel. This option appears only if `action` is `ipsec`.

Syntax:

```
set natoutbound {enable | disable}
```

Default value: `disable`

wccp

Enables or disables Web Cache Coordination Protocol (WCCP). If enabled, the traffic accepted by this policy is sent to a configured WCCP server as configured by the `config system wccp` command.

Syntax:

```
set wccp {enable|disable}
```

Default value: disable

ntlm

Enables or disables Directory Service authentication via NTLM. If you enable this option, you must also define the user groups. This field is available only if the `groups` or `users` fields are specified.

Syntax:

```
set ntlm {enable|disable}
```

Default value: disable

ntlm-guest

Enables or disables NTLM guest user access.

Syntax:

```
set ntlm-guest {enable|disable}
```

Default value: disable

ntlm-enabled-browsers

Sets the value for the HTTP-User-Agent of supported browsers. Enclose each string in quotes and separate strings with a space. Browsers with non-matching strings get guest access.

Syntax:

```
{set|append|clear} ntlm-enabled-browsers <user_agent_string>
```

fssso

Enables or disables Fortinet Single Sign On. This field is available when `groups` is populated.

Syntax:

```
set fssso {enable|disable}
```

Default value: disable

WSSO

Enables or disables WiFi Single Sign On.

Syntax:

```
set wssso {enable|disable}
```

Default value: disable

rssso

Enables or disables RADIUS-based single sign-on (SSO) for this policy.

Syntax:

```
set rssso {enable|disable}
```

Default value: disable

fssso-agent-for-ntlm

Specify FSSO agent for NTLM authentication.

Syntax:

```
set fssso-agent-for-ntlm <string>
```

groups

A listing of the names of the user groups allowed to use this policy. Separate multiple groups with a space.

Syntax:

```
{set|append} groups <user-group_object> [<user-group_object> ...]
```

Examples:

```
config firewall policy
  edit 0
  set groups group1
  or ...
  set groups group2 "Group 3"
  or ...
  append groups group4
end
```

users

A listing of the names of the users allowed to use this policy. Separate multiple users with a space.

Syntax:

```
{set|append} users <user_object> [<user_object> ...]
```

Examples:

```
config firewall policy
  edit 0
  set users adam
  or ...
  set users burt "Charlie C"
  or ...
  append users david
end
```

devices

A listing of of the names of devices or device categories that apply to this policy. Separate multiple devices with a space.

Syntax:

```
{set|append} devices <device_object> [<device_object> ...]
```

Examples:

```
config firewall policy
    edit 0
    set devices "adams pc"
    or ...
    set user bob-pc linux-pc
    or ...
    append user windows-pc
end
```

auth-path

Enables or disables authentication-based routing. You must also specify a RADIUS server, and the RADIUS server must be configured to supply the name of an object specified in `config router auth-path`. For details on configuring authentication-based routes, see `router auth-path`. This field is available only when the FortiGate unit is operating in NAT mode and the `groups` or `users` fields are specified.

Syntax:

```
set auth-path {enable|disable}
```

Default value: disable

disclaimer

Enables or disables the display of the authentication disclaimer page, which is configured with other replacement messages. The user must accept the disclaimer to connect to the destination.

Syntax:

```
set disclaimer {enable|disable}
```

Default value: disable

vpntunnel

Sets the name of a Phase 1 IPsec VPN configuration to apply to the IPsec tunnel. This field is available only if `action` is `ipsec`.

Syntax:

```
set vpntunnel <string>
```

Example:

```
config firewall policy
    edit 0
        set vpntunnel "TunnelA Phase 1"
    end
```

natip

Used to specify the source IP address and subnet mask to apply to outbound clear text packets before they are sent through the tunnel. If you do not specify a `natip` value when `natoutbound` is enabled, the source addresses of outbound encrypted packets are translated into the IP address of the FortiGate unit's external interface. When a `natip` value is specified, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate the source addresses of outbound IP packets into corresponding IP addresses on the subnetwork that you specify. For example, if the source address in the firewall encryption policy is 192.168.1.0/24 and the `natip` value is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7. This field is available only if `ipsec` and `natoutbound` is enabled.

Syntax:

```
set natip <IP_address> <IPv4mask>
```

match-vip

Enables or disables the function of matching DNATed packets. If you want to explicitly drop a packet that is not matched with a firewall policy and write a log message when this happens, you can add a general policy (source and destination address set to ANY) to the bottom of a policy list and configure the firewall policy to DENY packets and record a log message when a packet is dropped. In some cases, when a virtual IP performs destination NAT (DNAT) on a packet, the translated packet may not be accepted by a firewall policy. If this happens, the packet is silently dropped and therefore not matched with the general policy at the bottom of the policy list. To catch these packets, enable `match-vip` in the general policy. Then the DNATed packets that are not matched by a VIP policy are matched with the general policy where they can be explicitly dropped and logged.

Syntax:

```
set match-vip {enable|disable}
```

Default value: disable

diffserv-forward

Enables or disables application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, `diffservcode-forward` also needs to be configured.

Syntax:

```
set diffserv-forward {enable|disable}
```

Default value: disable

diffserv-reverse

Enables or disables application of the differentiated services code point (DSCP) value to the DSCP field of reverse (reply) traffic. If enabled, `diffservcode-rev` also needs to be configured.

Syntax:

```
set diffserv-reverse {enable | disable}
```

Default value: disable

diffservcode-forward

Used to set the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-forward` is enabled.

Syntax:

```
set diffservcode-forward <binary>
```

Default value: 000000

Example:

```
config firewall policy
    edit 0
        set diffservcode-forward 001001
    end
```

diffservcode-rev

Used to set the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-rev` is enabled.

Syntax:

```
set diffservcode-rev <binary>
```

Default value: 000000

tcp-mss-sender

Used to set the TCP Maximum Segment Size (MSS) number for the sender. When a FortiGate unit is configured to use PPPoE to connect to an ISP, certain web sites may not be accessible to users. This occurs because a PPPoE frame takes an extra 8 bytes off the standard Ethernet MTU of 1500. When the server sends the large packet with DF bit set to 1, the ADSL provider's router either does not send an "ICMP fragmentation needed" packet or the packet is dropped along the path to the web server. In either case, the web server never knows fragmentation is required to reach the client. Used to set the TCP Maximum Segment Size (MSS) number for the sender. When a FortiGate unit is configured to use PPPoE to connect to an ISP, certain web sites may not be accessible to users. This occurs because a PPPoE frame takes an extra 8 bytes off the standard Ethernet MTU of 1500. When the server sends the large packet with DF bit set to 1, the ADSL provider's router either does not send an "ICMP fragmentation needed" packet or the packet is dropped along the path to the web server. In either case, the web server never knows fragmentation is required to reach the client.

Syntax:

```
set tcp-mss-sender <integer>
```

tcp-mss-receiver

Used to set the TCP MSS number for the receiver.

Syntax:

```
set tcp-mss-receiver <integer>
```

Default value: 0

comments

Field to store descriptive information about the policy such as its intended purpose and targets. The field is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces.

Syntax:

```
set comments <string>
```

Default value: 0

Example:

```
config firewall policy
    edit 0
        set comments "Default outgoing traffic policy for corporate users"
    end
```

label

Used to set a label for this policy. The label is visible in the GUI in Section View.

Syntax:

```
set label <string>
```

global-label

Puts policy in the named subsection in the web-based manager. Subsection is created if it does not already exist.

Syntax:

```
set global-label <string>
```

auth-cert

Used to select an HTTPS server certificate for policy authentication. `self-sign` is the built-in, self-signed certificate; if you have added other certificates, you may select them instead. This field is available only if the `groups` or `users` fields are specified.

Syntax:

```
set auth-cert <string>
```

auth-redirect-addr

Used to set the IP address or domain name to redirect user HTTP requests after accepting the authentication disclaimer. The redirect URL could be to a web page with extra information (for example, terms of usage). To prevent web browser security warnings, this should match the CN field of the specified `auth-cert`, which is usually a fully qualified domain name (FQDN). This field is available only if the `groups` or `users` fields are specified.

Syntax:

```
set auth-redirect-addr <string>
```

redirect-url

Set the URL, if any, that the user is redirected to after authenticating and/or accepting the user authentication disclaimer. This field is available only if `disclaimer` is set to `enable`.

Syntax:

```
set redirect-url <string>
```

identity-based-route

Used to specify an identity-based route to be associated with the policy. Identity-based routes are defined in `firewall identity-based-route`.

Syntax:

```
set identity-based-route <string>
```

block-notification

Enables or disables the feature that displays the Fortinet Bar in the browser when a site is blocked and provides a block page via HTTP/HTTPS.

Syntax:

```
set block-notification {enable|disable}
```

Default value: disable

custom-log-fields

Used to enter log field index numbers to append one or more custom log fields to the log message for this policy. This option takes effect only if logging is enabled for the policy, and requires that you first define custom log fields. Separate multiple values with a space.

Syntax:

```
{set|append|clear} custom-log-fields <string> [<string> ...]
```

tags

Used to assign a custom tag to the firewall policy. The tags need to be preconfigured in `config system object-tag` and the same list of tags can be used anywhere that the tag setting is available. To see what tags are available for use, use the command `set tags ?`. Separate multiple values with a space.

Syntax:

```
{set|append|clear} tags <name_of_tag>
```

Example:

```
config system object-tag
  edit example-tag1
  next
  edit example-tag2
  next
  edit "example tag 3"
  next
```

```
end

config firewall policy
    edit 5
        set tags example-tag1 example-tag2
        append "example tag 3"
end
```

replacemsg-override-group

Used to select a replacement message override group from the available configured groups. This will override the default replacement message for this policy.

Syntax:

```
set replacemsg-override-group <string>
```

srcaddr-negate

Enables or disables the negate source address match function. When enabled, this causes the `srcaddr` field to specify what the source address must **not** be.

Syntax:

```
set srcaddr-negate {enable|disable}
```

Default value: disable

dstaddr-negate

Enables or disables the negate destination address match function. When enabled, this causes the `dstaddr` field to specify what the destination address must **not** be.

Syntax:

```
set dstaddr-negate {enable|disable}
```

Default value: disable

service-negate

Enables or disables the negate service match function. When enabled, this causes the `service` field to specify what the service traffic must **not** be.

Syntax:

```
set service-negate {enable|disable}
```

Default value: `disable`

timeout-send-rst

Enables or disables the sending of RST packet upon TCP session expiration.

Syntax:

```
set timeout-send-rst {enable|disable}
```

Default value: `disable`

captive-portal-exempt

Enables or disables the exemption of users of this policy from the captive portal interface.

Syntax:

```
set captive-portal-exempt {enable|disable}
```

Default value: `disable`

ssl-mirror

Enables or disables the SSL mirror function. This feature sends a copy of traffic decrypted by SSL inspection to one or more FortiGate interfaces so that it can be collected by raw packet capture tool for archiving and analysis. This feature is only available if the inspection mode is set do flow-based. Enables or disables the SSL mirror function. This feature sends a copy of traffic decrypted by SSL inspection to one or more FortiGate interfaces so that it can be collected by raw packet capture tool for archiving and analysis. This feature is only available if the inspection mode is set do flow-based.

Syntax:

```
set ssl-mirror {enable|disable}
```

Default value: disable

ssl-mirror-intf

Used to set the name of the SSL interface mirror. The value must be one of the existing interface names.

Syntax:

```
{set|append|clear} ssl-mirror-intf <string> [<string> ...]
```

Example:

```
config firewall policy
  edit 0
    set ssl-mirror-intf port11
  or ...
  set ssl-mirror-intf port12 port13
  or ...
  append ssl-mirror-intf port14
end
```

scan-botnet-connections

Sets the scanning level traffic for connections to Botnet servers.

Syntax:

```
set scan-botnet-connections {disable | block | monitor}
```

Default value: disable

dsri

Enables or disables Disable Server Response Inspection (DSRI) which is used to assist performance when only using URL filtering as it allows the system to ignore the HTTP server responses.

Syntax:

```
set dsri {enable|disable}
```

Default value: disable

delay-tcp-npu-sessoin

Enables or disables the TCP NPU session delay in order to guarantee packet order of 3-way handshake.

Syntax:

```
set delay-tcp-npu-sessoin {enable|disable}
```

Default value: disable

firewall {policy46 | policy64}

Introduction.

```

config firewall policy46
  edit { policyid }
  # Configure IPv4 to IPv6 policies.
  set permit-any-host { enable | disable }  Enable/disable allowing any host.
  set policyid { integer }  Policy ID. range[0-4294967294]
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set srcintf { string }  Source interface name. size[35] - datasource(s): system.zone.name,system.interface.name
  set dstintf { string }  Destination interface name. size[35] - datasource(s): system.interface.name,system.zone.name
  config srcaddr
    edit { name }
    # Source address objects.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstaddr
    edit { name }
    # Destination address objects.
    set name { string }  Address name. size[64] - datasource(s): firewall.vip46.name,firewall.vipgrp46.name
  next
  set action { accept | deny }  Accept or deny traffic matching the policy.
    accept  Accept matching traffic.
    deny    Deny matching traffic.
  set status { enable | disable }  Enable/disable this policy.
  set schedule { string }  Schedule name. size[35] - datasource(s): fire-
wall.schedule.onetime.name,firewall.schedule.recurring.name,firewall.schedule.group.name
  config service
    edit { name }
    # Service name.
    set name { string }  Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
  set logtraffic { enable | disable }  Enable/disable traffic logging for this policy.
  set traffic-shaper { string }  Traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
  set traffic-shaper-reverse { string }  Reverse traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
  set per-ip-shaper { string }  Per IP traffic shaper. size[35] - datasource(s): firewall.shaper.per-ip-shaper.name
  set fixedport { enable | disable }  Enable/disable fixed port for this policy.
  set tcp-mss-sender { integer }  TCP Maximum Segment Size value of sender (0 - 65535, default = 0). range[0-65535]

```

```
set tcp-mss-receiver { integer } TCP Maximum Segment Size value of receiver (0 - 65535, default = 0) range[0-65535]
set comments { string } Comment. size[1023]
config tags
  edit { name }
    # Applied object tags.
    set name { string } Names of object-tags (as configured in config system object-tag) applied to address. size[64] - datasource(s):
system.object-tag.name
  next
next
end

config firewall policy64
  edit { policyid }
    # Configure IPv6 to IPv4 policies.
    set policyid { integer } Policy ID. range[0-4294967294]
    set uuid { uuid } Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
    set srcintf { string } Source interface name. size[35] - datasource(s): system.zone.name,system.interface.name
    set dstintf { string } Destination interface name. size[35] - datasource(s): system.interface.name,system.zone.name
    config srcaddr
      edit { name }
        # Source address name.
        set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
      next
    config dstaddr
      edit { name }
        # Destination address name.
        set name { string } Address name. size[64] - datasource(s): fire-
wall.address.name,firewall.addrgrp.name,firewall.vip64.name,firewall.vipgrp64.name
      next
    set action { accept | deny } Policy action.
      accept Action accept.
      deny Action deny.
    set status { enable | disable } Enable/disable policy status.
    set schedule { string } Schedule name. size[35] - datasource(s): fire-
wall.schedule.onetime.name,firewall.schedule.recurring.name,firewall.schedule.group.name
    config service
      edit { name }
        # Service name.
        set name { string } Address name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
      next
    set logtraffic { enable | disable } Enable/disable policy log traffic.
    set permit-any-host { enable | disable } Enable/disable permit any host in.
```

```
set traffic-shaper { string } Traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set traffic-shaper-reverse { string } Reverse traffic shaper. size[35] - datasource(s): firewall.shaper.traffic-shaper.name
set per-ip-shaper { string } Per-IP traffic shaper. size[35] - datasource(s): firewall.shaper.per-ip-shaper.name
set fixedport { enable | disable } Enable/disable policy fixed port.
set ippool { enable | disable } Enable/disable policy64 IP pool.
config poolname
  edit { name }
  # Policy IP pool names.
  set name { string } IP pool name. size[64] - datasource(s): firewall.ippool.name
  next
set tcp-mss-sender { integer } TCP MSS value of sender. range[0-65535]
set tcp-mss-receiver { integer } TCP MSS value of receiver. range[0-65535]
set comments { string } Comment. size[1023]
config tags
  edit { name }
  # Applied object tags.
  set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
next
end
```

firewall profile-group

Introduction.

```
config firewall profile-group
  edit { name }
  # Configure profile groups.
  set name { string } Profile group name. size[35]
  set av-profile { string } Name of an existing Antivirus profile. size[35] - datasource(s): antivirus.profile.name
  set webfilter-profile { string } Name of an existing Web filter profile. size[35] - datasource(s): webfilter.profile.name
  set dnsfilter-profile { string } Name of an existing DNS filter profile. size[35] - datasource(s): dnsfilter.profile.name
  set spamfilter-profile { string } Name of an existing Spam filter profile. size[35] - datasource(s): spamfilter.profile.name
  set dlp-sensor { string } Name of an existing DLP sensor. size[35] - datasource(s): dlp.sensor.name
  set ips-sensor { string } Name of an existing IPS sensor. size[35] - datasource(s): ips.sensor.name
  set application-list { string } Name of an existing Application list. size[35] - datasource(s): application.list.name
  set voip-profile { string } Name of an existing VoIP profile. size[35] - datasource(s): voip.profile.name
  set icap-profile { string } Name of an existing ICAP profile. size[35] - datasource(s): icap.profile.name
  set waf-profile { string } Name of an existing Web application firewall profile. size[35] - datasource(s): waf.profile.name
  set profile-protocol-options { string } Name of an existing Protocol options profile. size[35] - datasource(s): firewall.profile-protocol-
options.name
  set ssl-ssh-profile { string } Name of an existing SSL SSH profile. size[35] - datasource(s): firewall.ssl-ssh-profile.name
  next
end
```

firewall profile-protocol-options

Use this command to configure protocol options.

```
config firewall profile-protocol-options
edit { name }
# Configure protocol options.
set name { string } Name. size[35]
set comment { string } Optional comments. size[255]
set replacemsg-group { string } Name of the replacement message group to be used size[35] - datasource(s): system.replacemsg-group.name
set oversize-log { disable | enable } Enable/disable logging for antivirus oversize file blocking.
set switching-protocols-log { disable | enable } Enable/disable logging for HTTP/HTTPS switching protocols.
set ports { integer } Ports to scan for content (1 - 65535, default = 80). range[1-65535]
set status { enable | disable } Enable/disable the active status of scanning for this protocol.
set inspect-all { enable | disable } Enable/disable the inspection of all ports for the protocol.
set options { clientcomfort | servercomfort | oversize | chunkedbypass } One or more options that can be applied to the session.
    clientcomfort Prevent client timeout.
    servercomfort Prevent server timeout.
    oversize Block oversized file/email.
    chunkedbypass Bypass chunked transfer encoded sites.
set comfort-interval { integer } Period of time between start, or last transmission, and the next client comfort transmission of data
(1 - 900 sec, default = 10). range[1-900]
set comfort-amount { integer } Amount of data to send in a transmission for client comforting (1 - 10240 bytes, default = 1). range[1-
10240]
set range-block { disable | enable } Enable/disable blocking of partial downloads.
set http-policy { disable | enable } Enable/disable HTTP policy check.
set post-lang { option } 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).
    jisx0201 Japanese Industrial Standard 0201.
    jisx0208 Japanese Industrial Standard 0208.
    jisx0212 Japanese Industrial Standard 0212.
    gb2312 Guojia Biaozhun 2312 (simplified Chinese).
    ksc5601-ex Wansung Korean standard 5601.
    euc-jp Extended Unicode Japanese.
    sjis Shift Japanese Industrial Standard.
    iso2022-jp ISO 2022 Japanese.
    iso2022-jp-1 ISO 2022-1 Japanese.
    iso2022-jp-2 ISO 2022-2 Japanese.
    euc-cn Extended Unicode Chinese.
```

```
ces-gbk      Extended GB2312 (simplified Chinese).
hz           Hanzi simplified Chinese.
ces-big5     Big-5 traditional Chinese.
euc-kr       Extended Unicode Korean.
iso2022-jp-3 ISO 2022-3 Japanese.
iso8859-1    ISO 8859 Part 1 (Western European).
tis620       Thai Industrial Standard 620.
cp874        Code Page 874 (Thai).
cp1252       Code Page 1252 (Western European Latin).
cp1251       Code Page 1251 (Cyrillic).
set fortinet-bar { enable | disable } Enable/disable Fortinet bar on HTML content.
set fortinet-bar-port { integer } Port for use by Fortinet Bar (1 - 65535, default = 8011). range[1-65535]
set streaming-content-bypass { enable | disable } Enable/disable bypassing of streaming content from buffering.
set switching-protocols { bypass | block } Bypass from scanning, or block a connection that attempts to switch protocol.
    bypass Bypass connections when switching protocols.
    block  Block connections when switching protocols.
set oversize-limit { integer } Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
set uncompressed-oversize-limit { integer } Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
set uncompressed-nest-limit { integer } Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
set scan-bzip2 { enable | disable } Enable/disable scanning of BZip2 compressed files.
set block-page-status-code { integer } Code number returned for blocked HTTP pages (non-FortiGuard only) (100 - 599, default = 200).
range[100-599]
set retry-count { integer } Number of attempts to retry HTTP connection (0 - 100, default = 0). range[0-100]
set ports { integer } Ports to scan for content (1 - 65535, default = 80). range[1-65535]
set status { enable | disable } Enable/disable the active status of scanning for this protocol.
set inspect-all { enable | disable } Enable/disable the inspection of all ports for the protocol.
set options { option } One or more options that can be applied to the session.
    clientcomfort Prevent client timeout.
    oversize       Block oversized file/email.
    splice         Enable splice mode.
    bypass-rest-command Bypass REST command.
    bypass-mode-command Bypass MODE command.
set comfort-interval { integer } Period of time between start, or last transmission, and the next client comfort transmission of data
(1 - 900 sec, default = 10). range[1-900]
set comfort-amount { integer } Amount of data to send in a transmission for client comforting (1 - 10240 bytes, default = 1). range[1-
10240]
set oversize-limit { integer } Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
set uncompressed-oversize-limit { integer } Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
set uncompressed-nest-limit { integer } Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
```

```

set scan-bzip2 { enable | disable } Enable/disable scanning of BZip2 compressed files.
set ports { integer } Ports to scan for content (1 - 65535, default = 80). range[1-65535]
set status { enable | disable } Enable/disable the active status of scanning for this protocol.
set inspect-all { enable | disable } Enable/disable the inspection of all ports for the protocol.
set options { fragmail | oversized } One or more options that can be applied to the session.
    fragmail Pass fragmented email.
    oversized Block oversized file/email.
set oversized-limit { integer } Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
set uncompressed-oversized-limit { integer } Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
set uncompressed-nest-limit { integer } Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
set scan-bzip2 { enable | disable } Enable/disable scanning of BZip2 compressed files.
set ports { integer } Ports to scan for content (1 - 65535, default = 80). range[1-65535]
set status { enable | disable } Enable/disable the active status of scanning for this protocol.
set options { fragmail | oversized } One or more options that can be applied to the session.
    fragmail Pass fragmented email.
    oversized Block oversized file/email.
set oversized-limit { integer } Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
set uncompressed-oversized-limit { integer } Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
set uncompressed-nest-limit { integer } Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
set scan-bzip2 { enable | disable } Enable/disable scanning of BZip2 compressed files.
set ports { integer } Ports to scan for content (1 - 65535, default = 80). range[1-65535]
set status { enable | disable } Enable/disable the active status of scanning for this protocol.
set inspect-all { enable | disable } Enable/disable the inspection of all ports for the protocol.
set options { fragmail | oversized } One or more options that can be applied to the session.
    fragmail Pass fragmented email.
    oversized Block oversized file/email.
set oversized-limit { integer } Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
set uncompressed-oversized-limit { integer } Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
set uncompressed-nest-limit { integer } Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
set scan-bzip2 { enable | disable } Enable/disable scanning of BZip2 compressed files.
set ports { integer } Ports to scan for content (1 - 65535, default = 80). range[1-65535]
set status { enable | disable } Enable/disable the active status of scanning for this protocol.
set inspect-all { enable | disable } Enable/disable the inspection of all ports for the protocol.
set options { fragmail | oversized | splice } One or more options that can be applied to the session.
    fragmail Pass fragmented email.
    oversized Block oversized file/email.
    splice Enable splice mode.

```

```
    set oversize-limit { integer }    Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
    set uncompressed-oversize-limit { integer }    Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
    set uncompressed-nest-limit { integer }    Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
    set scan-bzip2 { enable | disable }    Enable/disable scanning of BZip2 compressed files.
    set server-busy { enable | disable }    Enable/disable SMTP server busy when server not available.
    set ports { integer }    Ports to scan for content (1 - 65535, default = 80). range[1-65535]
    set status { enable | disable }    Enable/disable the active status of scanning for this protocol.
    set inspect-all { enable | disable }    Enable/disable the inspection of all ports for the protocol.
    set options { oversize | splice }    One or more options that can be applied to the session.
        oversize    Block oversized file/email.
        splice    Enable splice mode.
    set oversize-limit { integer }    Maximum in-memory file size that can be scanned (1 - 383 MB, default = 10). range[1-1606]
    set uncompressed-oversize-limit { integer }    Maximum in-memory uncompressed file size that can be scanned (0 - 383 MB, 0 = unlimited,
default = 10). range[0-1606]
    set uncompressed-nest-limit { integer }    Maximum nested levels of compression that can be uncompressed and scanned (2 - 100, default =
12). range[2-100]
    set scan-bzip2 { enable | disable }    Enable/disable scanning of BZip2 compressed files.
    set ports { integer }    Ports to scan for content (1 - 65535, default = 80). range[1-65535]
    set status { enable | disable }    Enable/disable the active status of scanning for this protocol.
    set status { disable | enable }    Enable/disable adding an email signature to SMTP email messages as they pass through the FortiGate.
    set signature { string }    Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation
marks). size[1023]
    set rpc-over-http { enable | disable }    Enable/disable inspection of RPC over HTTP.
    next
end
```


firewall proxy-address

Introduction.

```
config firewall proxy-address
  edit { name }
    # Web proxy address configuration.
    set name { string }   Address name. size[35]
    set uuid { uuid }     Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
    set type { option }   Proxy address type.
      host-regex          Host regular expression.
      url                  HTTP URL.
      category             FortiGuard URL category.
      method               HTTP request method.
      ua                   HTTP request user agent.
      header               HTTP request header.
      src-advanced         HTTP advanced source criteria.
      dst-advanced         HTTP advanced destination criteria.
    set host { string }   Address object for the host. size[63] - datasource(s): firewall.address.name, firewall.addrgrp.name, firewall.proxy-address.name
    set host-regex { string } Host name as a regular expression. size[255]
    set path { string }   URL path as a regular expression. size[255]
    config category
      edit { id }
        # FortiGuard category ID.
        set id { integer } FortiGuard category id. range[0-4294967295]
      next
    set method { option } HTTP request methods to be used.
      get                  GET method.
      post                 POST method.
      put                  PUT method.
      head                 HEAD method.
      connect              CONNECT method.
      trace                TRACE method.
      options              OPTIONS method.
      delete               DELETE method.
    set ua { option }    Names of browsers to be used as user agent.
      chrome               Google Chrome.
      ms                   Microsoft Internet Explorer or EDGE.
```

```
        firefox Mozilla Firefox.
        safari  Apple Safari.
        other   Other browsers.
set header-name { string } Name of HTTP header. size[79]
set header { string } HTTP header name as a regular expression. size[255]
set case-sensitivity { disable | enable } Enable to make the pattern case sensitive.
config header-group
    edit { id }
        # HTTP header group.
        set id { integer } ID. range[0-4294967295]
        set header-name { string } HTTP header. size[79]
        set header { string } HTTP header regular expression. size[255]
        set case-sensitivity { disable | enable } Case sensitivity in pattern.
    next
set color { integer } Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1). range[0-32]
config tags
    edit { name }
        # Names of object-tags (as configured in config system object-tag) applied to address.
        set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
    next
set comment { string } Optional comments. size[255]
set visibility { enable | disable } Enable/disable visibility of the object in the GUI.
next
end
```

firewall proxy-addrgrp

Introduction.

```
config firewall proxy-addrgrp
  edit { name }
  # Web proxy address group configuration.
  set name { string }  Address group name. size[63]
  set type { src | dst }  Source or destination address group type.
    src Source group.
    dst Destination group.
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  config member
    edit { name }
    # Members of address group.
    set name { string }  Address name. size[64] - datasource(s): firewall.proxy-address.name,firewall.proxy-addrgrp.name
    next
  set color { integer }  Integer value to determine the color of the icon in the GUI (1 - 32, default = 0, which sets value to 1). range[0-32]
  config tags
    edit { name }
    # Names of object-tags (as configured in config system object-tag) applied to address.
    set name { string }  Tag name. size[64] - datasource(s): system.object-tag.name
    next
  set comment { string }  Optional comments. size[255]
  set visibility { enable | disable }  Enable/disable visibility of the object in the GUI.
  next
end
```

firewall proxy-policy

Introduction.

```
config firewall proxy-policy
  edit { policyid }
  # Configure proxy policies.
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set policyid { integer }  Policy ID. range[0-4294967295]
  set proxy { explicit-web | transparent-web | ftp | wanopt }  Type of explicit proxy.
    explicit-web  Explicit Web Proxy
    transparent-web  Transparent Web Proxy
    ftp  Explicit FTP Proxy
    wanopt  WANopt Tunnel
  config srcintf
    edit { name }
    # Source interface names.
    set name { string }  Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
  config dstintf
    edit { name }
    # Destination interface names.
    set name { string }  Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
  next
  config srcaddr
    edit { name }
    # Source address objects (must be set when using Web proxy).
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name,firewall.proxy-address.-
name,firewall.proxy-addrgrp.name
  next
  config poolname
    edit { name }
    # Name of IP pool object.
    set name { string }  IP pool name. size[64] - datasource(s): firewall.ippool.name
  next
  config dstaddr
    edit { name }
    # Destination address objects.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name,firewall.proxy-
```

```

address.name, firewall.proxy-addrgrp.name, firewall.vip.name, firewall.vipgrp.name, firewall.vip46.name, firewall.vipgrp46.name
    next
    set internet-service { enable | disable } Enable/disable use of Internet Services for this policy. If enabled, destination address and ser-
vice are not used.
    set internet-service-negate { enable | disable } When enabled, Internet Services match against any internet service EXCEPT the selected
Internet Service.
    config internet-service-id
        edit { id }
        # Internet Service ID.
        set id { integer } Internet Service ID. range[0-4294967295] - datasource(s): firewall.internet-service.id
    next
    config internet-service-custom
        edit { name }
        # Custom Internet Service name.
        set name { string } Custom name. size[64] - datasource(s): firewall.internet-service-custom.name
    next
    config service
        edit { name }
        # Name of service objects.
        set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name, firewall.service.group.name
    next
    set srcaddr-negate { enable | disable } When enabled, source addresses match against any address EXCEPT the specified source addresses.
    set dstaddr-negate { enable | disable } When enabled, destination addresses match against any address EXCEPT the specified destination
addresses.
    set service-negate { enable | disable } When enabled, services match against any service EXCEPT the specified destination services.
    set action { accept | deny | redirect } Accept or deny traffic matching the policy parameters.
        accept Action accept.
        deny Action deny.
        redirect Action redirect.
    set status { enable | disable } Enable/disable the active status of the policy.
    set schedule { string } Name of schedule object. size[35] - datasource(s): fire-
wall.schedule.onetime.name, firewall.schedule.recurring.name, firewall.schedule.group.name
    set logtraffic { all | utm | disable } Enable/disable logging traffic through the policy.
        all Log all sessions.
        utm UTM event and matched application traffic log.
        disable Disable traffic and application log.
    config srcaddr6
        edit { name }
        # IPv6 source address objects.
        set name { string } Address name. size[64] - datasource(s): firewall.address6.name, firewall.addrgrp6.name
    next
    config dstaddr6
        edit { name }

```

```

    # IPv6 destination address objects.
    set name { string } Address name. size[64] - datasource(s): fire-
wall.address6.name, firewall.addrgrp6.name, firewall.vip6.name, firewall.vipgrp6.name, firewall.vip64.name, firewall.vipgrp64.name
    next
config groups
  edit { name }
  # Names of group objects.
  set name { string } Group name. size[64] - datasource(s): user.group.name
  next
config users
  edit { name }
  # Names of user objects.
  set name { string } Group name. size[64] - datasource(s): user.local.name
  next
set webproxy-forward-server { string } Name of web proxy forward server. size[63] - datasource(s): web-proxy.forward-server.name, web-proxy.-
forward-server-group.name
set webproxy-profile { string } Name of web proxy profile. size[63] - datasource(s): web-proxy.profile.name
set transparent { enable | disable } Enable to use the IP address of the client to connect to the server.
set webcache { enable | disable } Enable/disable web caching.
set webcache-https { disable | enable } Enable/disable web caching for HTTPS (Requires deep-inspection enabled in ssl-ssh-profile).
set disclaimer { disable | domain | policy | user } Web proxy disclaimer setting: by domain, policy, or user.
    disable Disable disclaimer.
    domain Display disclaimer for domain
    policy Display disclaimer for policy
    user Display disclaimer for current user
set utm-status { enable | disable } Enable the use of UTM profiles/sensors/lists.
set profile-type { single | group } Determine whether the firewall policy allows security profile groups or single profiles only.
    single Do not allow security profile groups.
    group Allow security profile groups.
set profile-group { string } Name of profile group. size[35] - datasource(s): firewall.profile-group.name
set av-profile { string } Name of an existing Antivirus profile. size[35] - datasource(s): antivirus.profile.name
set webfilter-profile { string } Name of an existing Web filter profile. size[35] - datasource(s): webfilter.profile.name
set spamfilter-profile { string } Name of an existing Spam filter profile. size[35] - datasource(s): spamfilter.profile.name
set dlp-sensor { string } Name of an existing DLP sensor. size[35] - datasource(s): dlp.sensor.name
set ips-sensor { string } Name of an existing IPS sensor. size[35] - datasource(s): ips.sensor.name
set application-list { string } Name of an existing Application list. size[35] - datasource(s): application.list.name
set icap-profile { string } Name of an existing ICAP profile. size[35] - datasource(s): icap.profile.name
set waf-profile { string } Name of an existing Web application firewall profile. size[35] - datasource(s): waf.profile.name
set profile-protocol-options { string } Name of an existing Protocol options profile. size[35] - datasource(s): firewall.profile-protocol-
options.name
set ssl-ssh-profile { string } Name of an existing SSL SSH profile. size[35] - datasource(s): firewall.ssl-ssh-profile.name
set replacemsg-override-group { string } Authentication replacement message override group. size[35] - datasource(s): system.replacemsg-
group.name

```

```
set logtraffic-start { enable | disable } Enable/disable policy log traffic start.
config tags
  edit { name }
    # Names of object-tags applied to address. Tags need to be preconfigured in config system object-tag. Separate multiple tags with a
space.
    set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
set label { string } VDOM-specific GUI visible label. size[63]
set global-label { string } Global web-based manager visible label. size[63]
set scan-botnet-connections { disable | block | monitor } Enable/disable scanning of connections to Botnet servers.
  disable Do not scan connections to botnet servers.
  block Block connections to botnet servers.
  monitor Log connections to botnet servers.
set comments { string } Optional comments. size[1023]
set redirect-url { string } Redirect URL for further explicit web proxy processing. size[1023]
next
end
```

firewall schedule group

This command is used to configure schedule groups.

```
config firewall schedule group
  edit { name }
  # Schedule group configuration.
  set name { string }  Schedule group name. size[31]
  config member
    edit { name }
    # Schedules added to the schedule group.
    set name { string }  Schedule name. size[64] - datasource(s): firewall.schedule.onetime.name, firewall.schedule.recurring.name
  next
  set color { integer }  Color of icon on the GUI. range[0-32]
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

Syntax

```
config firewall schedule group {edit|delete|purge|rename|get|show}
```

Managing schedule group objects

The configuration of specific schedule group objects is the most common activity when using the `config firewall schedule group` command but some commands affect the address objects as a whole.

edit

Used to select which individual schedule group to configure or edit values.

```
edit <schedule group>
```


To get a list of all of the existing schedule group objects, type the command:

```
Command Prompt (group) # edit ?
```

If you are creating a new schedule group object, just type the name you wish to use after the edit command. If there are spaces in the name, use quotation marks.

delete

Used to delete an existing schedule object

```
delete
```

The can be a string of up to 64 characters.

purge

Used delete all of the existing schedule group objects. It deletes all of the values within the table that holds the information about schedule group objects within the VDOM.

```
purge
```

There are no options, parameters or qualifiers. Just use the enter key after entering the command This command has a serious impact. Use cautiously.

rename

Used to change the name of the schedule group object.

```
rename <schedule group> to <schedule group>
```

Options and settings within a Schedule Group

name

This field is a unique name given to represent the schedule group object. This setting is first defined when using the edit command to edit a category that does not currently exist. The name field of a schedule group object cannot be changed from within the object. It can be changed by using the rename command in the config firewall schedule group context.

member

Defines the schedule objects that are members of the schedule group. The value is a that should be the name of one of the existing schedule objects configured on the device. A group cannot contain other groups Separate multiple interfaces with spaces.

Syntax:

```
{set|append} members <schedule group>[ ...]
```

Example:

```
config firewall schedule group
  edit example_group
  set member example_schedule1
  or ...
  set member example_schedule1 example_schedule2
  or ...
  append example_schedule3
end
```

color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1.

Syntax:

```
set color <integer>
```

Default value: 0

Example:

```
config firewall schedule group
  edit generic-schedule group-name
  set color 15
end
```

firewall schedule onetime

This command is used to add, edit, delete or rename one-time schedules.

Schedule objects are used to control when policies are active or inactive. The one-time schedule is for policies that are effective once for a specified period of time and then not used again.

```
config firewall schedule onetime
  edit { name }
  # Onetime schedule configuration.
  set name { string }    Onetime schedule name. size[31]
  set start { string }  Schedule start date and time, format hh:mm yyyy/mm/dd.
  set end { string }    Schedule end date and time, format hh:mm yyyy/mm/dd.
  set color { integer } Color of icon on the GUI. range[0-32]
  set expiration-days { integer } Write an event log message this many days before the schedule expires. range[0-100]
  next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

Syntax

```
config firewall schedule onetime {edit|delete|purge|rename|get|show}
```

Managing service group objects

The configuration of a specific onetime schedule object is the most common activity when using the `config firewall schedule onetime` command but some commands affect the schedule objects as a whole.

edit

Used to select which individual schedule to configure or edit values.

```
edit <onetime schedule>
```

To get a list of all of the existing service group objects, type the command:

```
Command Prompt (onetime) # edit ?
```

If you are creating a new onetime schedule object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

delete

Used to delete an existing onetime schedule

```
delete <onetime schedule>
```

- The `<onetime schedule>` can be a string of up to 64 characters.

purge

Used to delete all of the existing onetime schedule objects. It deletes all of the values within the table that holds the information about service group objects within the VDOM.

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

rename

Used to change the name of the onetime schedule object.

```
rename <onetime schedule> to <new_onetime_schedule>
```

Options and settings within a onetime schedule

name

This field is a unique name given to represent the onetime schedule object. This setting is first defined when using the `edit` command to edit a category that does not currently exist. The name field of a onetime schedule object cannot be changed from within the object. It can be changed by using the `rename` command in the `config firewall schedule onetime` context.

start

This field is for specifying the starting date and time of the schedule object.

Syntax:

```
<hh:mm> <yyyy/mm/dd>
```

- `hh` - hours in the 24-hour clock: 00 to 23
- `mm` - Minutes in quarter hour increments: 15, 30, or 45
- `yyyy` - Year, the range being: 2001-2050
- `mm` - Months: 01 to 12
- `dd` - Day of the month: 01 to 31

Default value: 00:00 2001/01/01

end

Enter the ending day and time of the schedule.

Syntax:

```
<hh:mm> <yyyy/mm/dd>
```

- `hh` - hours in the 24-hour clock: 00 to 23
- `mm` - Minutes in quarter hour increments: 15, 30, or 45
- `yyyy` - Year, the range being: 2001-2050
- `mm` - Months: 01 to 12
- `dd` - Day of the month: 01 to 31

Default value: 00:00 2001/01/01

Example of setting the times

- Set the start time to 1:30 p.m. on August 4, 2018
- Set the end time to 12:45 a.m. on August 31, 2018

```
config firewall schedule onetime
  edit schedule1
    set start 13:30 2018/08/04
```

```
        set end 00:45 2018/08/31
end
```

color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1.

Syntax

```
set color <integer>
```

Default value: 0

Example:

```
config firewall schedule onetime
    edit schedule1
        set color 15
end
```

expiration-days

This field specifies how many days before the expiration of the schedule an event log will be generated in order to warn of the impending cancellation of the schedule. The content of the field is an integer. To generate an event, the range is 1 to 100 days. To disable the generation of the event log, enter 0.

Example

```
config firewall schedule onetime
    edit schedule1
        set expiration-days 5
end
```

Default value: 3

firewall schedule recurring

Introduction.

```
config firewall schedule recurring
  edit { name }
  # Recurring schedule configuration.
  set name { string }   Recurring schedule name. size[31]
  set start { string }  Time of day to start the schedule, format hh:mm.
  set end { string }    Time of day to end the schedule, format hh:mm.
  set day { option }    One or more days of the week on which the schedule is valid. Separate the names of the days with a space.
    sunday      Sunday.
    monday      Monday.
    tuesday     Tuesday.
    wednesday   Wednesday.
    thursday    Thursday.
    friday      Friday.
    saturday    Saturday.
    none        None.
  set color { integer } Color of icon on the GUI. range[0-32]
next
end
```

firewall service category

Use this command to create new categories or add comments to firewall service categories. To assign services to categories, use the `firewall service custom` command. The adding or editing the name of a service category are the most common tasks when using the `config firewall service category` command but some commands affect the address objects as a whole.

```
config firewall service category
  edit { name }
  # Configure service categories.
  set name { string }  Service category name. size[63]
  set comment { string }  Comment. size[255]
  next
end
```

edit

Used to add an additional category or select which individual category to edit.

Syntax:

```
edit <category_name>
```

To create a new service category, just type the `category_name` you wish to use after the `edit` command. A new category will be created using the `category_name` supplied. If you require spaces in the name you can:

- Use quotation marks around the entire `category_name`
- Use the escape character before the space character. Example: for the `category_name` `Web Access` type `Web\ Access`

To get a list of all of the existing categories, type the command:

```
Command Prompt (category) # edit ?
```

delete

Used to delete an existing category

Syntax:

```
delete <category_name>
```

purge

Used delete all of the existing categories. It deletes all of the values within the table that holds the categories.

Syntax:

```
purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

rename

Used to change the name of the category.

Syntax:

```
rename <category_name> to <new_category_name>
```

move

Used to move the position of a category, relative to another category, in the order of their listing.

Syntax:

```
move <category_name> {after | before} <category_name>
```

clone

Used to copy all of the attributes of an existing category to a new category.

Syntax:

```
clone <category_name> to <category_name>
```

name

This field is a unique name given to represent the address object. This setting is first defined when using the edit command to edit a category that does not currently exist. The name field of an address object cannot be changed from within the object. It can be changed by using the rename command in the `config firewall service category` context.

comment

Field used to store descriptive information about the category such as the type of services that should be included in the category. Enclose the string in quotes to enter special characters or spaces.

Syntax:

```
set comment <string>
```

Example:

```
config firewall service category
  edit "Custom Category"
    set comment "For services that are proprietary to the company."
end
```

firewall service custom

This command is used to configure firewall services.

```
config firewall service custom
edit { name }
# Configure custom services.
set name { string } Custom service name. size[63]
set proxy { enable | disable } Enable/disable web proxy service.
set category { string } Service category. size[63] - datasource(s): firewall.service.category.name
set protocol { option } Protocol type based on IANA numbers.
    TCP/UDP/SCTP TCP, UDP and SCTP.
    ICMP ICMP.
    ICMP6 ICMP6.
    IP IP.
    HTTP HTTP - for web proxy.
    FTP FTP - for web proxy.
    CONNECT Connect - for web proxy.
    SOCKS-TCP Socks TCP - for web proxy.
    SOCKS-UDP Socks UDP - for web proxy.
    ALL All - for web proxy.
set helper { option } Helper name.
    auto Automatically select helper based on protocol and port.
    disable Disable helper.
    ftp FTP.
    tftp TFTP.
    ras RAS.
    h323 H323.
    tns TNS.
    mms MMS.
    sip SIP.
    pptp PPTP.
    rtsp RTSP.
    dns-udp DNS UDP.
    dns-tcp DNS TCP.
    pmap PMAP.
    rsh RSH.
    dcerpc DCERPC.
    mgcp MGCP.
```

```

set iprange { string } Start and end of the IP range associated with service.
set fqdn { string } Fully qualified domain name. size[255]
set protocol-number { integer } IP protocol number. range[0-254]
set icmp-type { integer } ICMP type. range[0-4294967295]
set icmp-code { integer } ICMP code. range[0-255]
set tcp-portrange { string } Multiple TCP port ranges.
set udp-portrange { string } Multiple UDP port ranges.
set sctp-portrange { string } Multiple SCTP port ranges.
set tcp-halfclose-timer { integer } Wait time to close a TCP session waiting for an unanswered FIN packet (1 - 86400 sec, 0 = default).
range[0-86400]
set tcp-halfopen-timer { integer } Wait time to close a TCP session waiting for an unanswered open session packet (1 - 86400 sec, 0 =
default). range[0-86400]
set tcp-timewait-timer { integer } Set the length of the TCP TIME-WAIT state in seconds (1 - 300 sec, 0 = default). range[0-300]
set udp-idle-timer { integer } UDP half close timeout (0 - 86400 sec, 0 = default). range[0-86400]
set session-ttl { integer } Session TTL (300 - 604800, 0 = default). range[300-604800]
set check-reset-range { disable | strict | default } Configure the type of ICMP error message verification.
    disable Disable RST range check.
    strict Check RST range strictly.
    default Using system default setting.
set comment { string } Comment. size[255]
set color { integer } Color of icon on the GUI. range[0-32]
set visibility { enable | disable } Enable/disable the visibility of the service on the GUI.
set app-service-type { disable | app-id | app-category } Application service type.
    disable Disable application type.
    app-id Application ID.
    app-category Application category.
config app-category
    edit { id }
        # Application category ID.
        set id { integer } Application category id. range[0-4294967295]
    next
config application
    edit { id }
        # Application ID.
        set id { integer } Application id. range[0-4294967295]
    next
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

Managing service objects

The configuration of specific service is the most common activity when using the firewall policy command but some commands affect the service objects as a whole.

edit

Used to select which individual service to configure or edit values.

Syntax:

```
config firewall service custom
(custom) # edit <service>
```

- To get a list of all of the existing address objects, type the command:

```
(custom) # edit ?
```

If you are creating a new service object, just type the name you wish to use after the `edit` command. If there are spaces in the name, use quotation marks.

delete

Used to delete an existing service

Syntax:

```
config firewall service custom
(custom) # delete <service>
```

purge

Used to delete all of the existing firewall policies. It deletes all of the values within the table within the VDOM.

Syntax:

```
config firewall service custom
(custom) # purge
```

- There are no options, parameters or qualifiers. Just use the enter key after entering the command
- This command has a serious impact. Use cautiously.

rename

Used to change the name of the service object.

```
config firewall service custom
(custom) # rename <service_name> to <new_service_name>
```

Options and settings within a service

explicit-proxy

Enable to configure this service as an explicit web proxy service. The service will be available to explicit proxy firewall policies but not to regular firewall policies.

Syntax

```
set explicit-proxy {enable | disable}
```

Default value: disable

category

Assign the service to a service category. These categories are created and managed using the command `firewall service`.

Syntax

```
set category <category_name>
```

Example

```
config firewall services custom
    (custom) # edit sample_service
        (sample_service) # set category "web services"
    (sample_service) # end
```

protocol

Select the protocol used by the service. These protocols are available when `explicit-proxy` is disabled. If you select `TCP/UDP/SCTP` you must specify the `tcp-portrange`, `udp-portrange`, or `sctp-portrange`.

Syntax

```
set protocol {ICMP | ICMP6 | IP | TCP/UDP/SCTP}
```

Default value: `TCP/UDP/SCTP` A different set of protocols are available when `explicit-proxy` is enabled.

```
set protocol {ALL | CONNECT | FTP | HTTP | SOCKS-TCP | SOCKS-UDP}
```

Default value: `ALL`

Example

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set explicit-proxy enable
    (sample-service) # set protocol FTP
(sample-service) # end
```

iprange

Enter an IP address or address range for this service.

Syntax

```
set iprange <ip_address[-<ip_address>]>
```

Default value: `0.0.0.0`

Example

```
config firewall service custom
    (custom) # edit sample-service
    (sample-service) # set iprange 192.168.0.64-192.168.0.128
(sample-service) # end
```

fqdn

Enter a fully-qualified domain name (FQDN) for this service.

Syntax

```
set fqdn <fqdn_str>
```

Example

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set fqdn example.com
    (sample-service) # end
```

protocol-number (0,4294967295)

For an IP service, enter the IP protocol number. For information on protocol numbers, see <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>.

Syntax

```
set protocol-number <protocol_int>
```

Default value: 0

Example

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set protocol-number 6
    (sample-service) # end
```

icmptype

Enter the ICMP type number. The range for type_int is from 0-255. Find ICMP type and code numbers at <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-types>.

Syntax

```
set icmptype <type_int>
```

Example

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set icmptype 8
    (sample-service) # end
```

icmpcode

Enter the ICMP code number. Find ICMP type and code numbers at <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-types>.

Syntax

```
set icmpcode <code_int>
```

Example

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set icmpcode 13
    (sample-service) # end
```

tcp-portrange

For TCP services, enter the destination and source port ranges.

- If the destination port range can be any port, enter 0–65535.
- If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`.
- If the source port can be any port, no source port need be added.
- If source port can be any port, no source port need be added.
- If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.

The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.

Syntax

```
set tcp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<srcporthigh_int>]
```

Example

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set tcp-portrange 100-150:1100-1150
    (sample-service) # end
```

or if multiple ranges, separate the ranges with a space.

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set tcp-portrange 100-150:1100-1150 2000-2100:4000:4100
    (sample-service) # end
```

udp-portrange

For UDP services, enter the destination and source port ranges.

- If the destination port range can be any port, enter 0-65535.
- If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`.
- If source port can be any port, no source port need be added.
- If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.

The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.

Syntax

```
set udp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<srcporthigh_int>]
```

sctp-portrange

For SCTP services, enter the destination and source port ranges.

- If the destination port range can be any port, enter 0-65535.
- If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`.

- If source port can be any port, no source port need be added.
- If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.

The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.

Syntax

```
set sctp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<srcporthigh_int>]
```

tcp-halfclose-timer (0,86400)

Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in `system global`. This is available when `protocol` is TCP/UDP/SCTP.

Syntax

```
set tcp-halfclose-timer <seconds>
```

Default value: 0

Example:

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set tcp-halfclose-timer 3600
    (sample-service) # end
```

tcp-halfopen-timer (0,86400)

Enter how many 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. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in `system global`. This is available when `protocol` is TCP/UDP/SCTP.

Syntax

```
set tcp-halfopen-timer <seconds>
```

Default value: 0

tcp-timewait-timer

Set the length of the TCP TIME-WAIT state in seconds. As described in [RFC 793](#), the “TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request”. Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds Enter 0 to use the global setting defined in system global. This is available when protocol is TCP/UDP/SCTP.

Syntax

```
set tcp-timewait-timer <seconds_int>
```

Default value: 0

Example:

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set tcp-timewait-timer 60
    (sample-service) # end
```

udp-idle-timer

Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in system global. This is available when protocol is TCP/UDP/SCTP.

Syntax

```
set udp-idle-timer <seconds>
```

Default value: 0

session-ttl

Enter the default session timeout in seconds. The valid range is from 300 - 604,800 seconds. Enter 0 to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. This is available when protocol is TCP/UDP/SCTP.

Syntax

```
set session-ttl <seconds>
```

Default value: 0

Example:

```
config firewall service custom
    (custom) # edit sample-service
        (sample-service) # set session-ttl 3600
    (sample-service) # end
```

check-reset-range

Configure ICMP error message verification.

- `disable` — The FortiGate unit does not validate ICMP error messages.
- `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If `log-invalid-packet` is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the anti-replay option checks packets.
- `default` — Use the global setting defined in system global.

This field is available when protocol is TCP/UDP/SCTP. This field is not available if explicit-proxy is enabled.

Syntax

```
set check-reset-range {disable | strict | default}
```

Default value: default

comment

Field to store descriptive information about the service such as its intended purpose.

Syntax

```
set comment <string>
```

color

This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1. This setting determines the color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. 0 will set the color to default which is color number 1.

Syntax

```
set color <integer>
```

Default value: 0

Example:

```
config firewall service custom
  edit generic-custom-service
    set color 15
end
```

visibility

Enable visibility to include this service in firewall policy service selection.

Syntax

```
set visibility {enable | disable}
```

Default value: enable

firewall service group

Introduction.

```
config firewall service group
  edit { name }
  # Configure service groups.
  set name { string }  Address group name. size[35]
  config member
    edit { name }
    # Service objects contained within the group.
    set name { string }  Address name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
    next
  set proxy { enable | disable }  Enable/disable web proxy service group.
  set comment { string }  Comment. size[255]
  set color { integer }  Color of icon on the GUI. range[0-32]
  next
end
```

firewall shaper per-ip-shaper

Introduction.

```
config firewall shaper per-ip-shaper
  edit { name }
    # Configure per-IP traffic shaper.
    set name { string } Traffic shaper name. size[35]
    set max-bandwidth { integer } Upper bandwidth limit enforced by this shaper (0 - 16776000). 0 means no limit. Units depend on the bandwidth-unit setting. range[0-16776000]
    set bandwidth-unit { kbps | mbps | gbps } Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).
      kbps Kilobits per second.
      mbps Megabits per second.
      gbps Gigabits per second.
    set max-concurrent-session { integer } Maximum number of concurrent sessions allowed by this shaper (0 - 2097000). 0 means no limit. range [0-2097000]
    set diffserv-forward { enable | disable } Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.
    set diffserv-reverse { enable | disable } Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.
    set diffservcode-forward { string } Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.
    set diffservcode-rev { string } Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.
  next
end
```


firewall shaper traffic-shaper

Introduction.

```
config firewall shaper traffic-shaper
  edit { name }
  # Configure shared traffic shaper.
  set name { string } Traffic shaper name. size[35]
  set guaranteed-bandwidth { integer } Amount of bandwidth guaranteed for this shaper (0 - 16776000). Units depend on the bandwidth-unit setting. range[0-16776000]
  set maximum-bandwidth { integer } Upper bandwidth limit enforced by this shaper (0 - 16776000). 0 means no limit. Units depend on the bandwidth-unit setting. range[0-16776000]
  set bandwidth-unit { kbps | mbps | gbps } Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).
    kbps Kilobits per second.
    mbps Megabits per second.
    gbps Gigabits per second.
  set priority { low | medium | high } Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.
    low Low priority.
    medium Medium priority.
    high High priority.
  set per-policy { disable | enable } Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.
  set diffserv { enable | disable } Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.
  set diffservcode { string } DiffServ setting to be applied to traffic accepted by this shaper.
next
end
```

firewall shaping-policy

Introduction.

```
config firewall shaping-policy
  edit { id }
  # Configure shaping policies.
  set id { integer }   Shaping policy ID. range[0-4294967295]
  set status { enable | disable }   Enable/disable this traffic shaping policy.
  set ip-version { 4 | 6 }   Apply this traffic shaping policy to IPv4 or IPv6 traffic.
    4 Use IPv4 addressing for Configuration Method.
    6 Use IPv6 addressing for Configuration Method.
  config srcaddr
    edit { name }
    # IPv4 source address and address group names.
    set name { string }   Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config dstaddr
    edit { name }
    # IPv4 destination address and address group names.
    set name { string }   Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config srcaddr6
    edit { name }
    # IPv6 source address and address group names.
    set name { string }   Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
  config dstaddr6
    edit { name }
    # IPv6 destination address and address group names.
    set name { string }   Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
  config service
    edit { name }
    # Service and service group names.
    set name { string }   Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
  config users
    edit { name }
```

```
# Apply this traffic shaping policy to individual users that have authenticated with the FortiGate.
    set name { string }    User name. size[64] - datasource(s): user.local.name
    next
config groups
    edit { name }
    # Apply this traffic shaping policy to user groups that have authenticated with the FortiGate.
        set name { string }    Group name. size[64] - datasource(s): user.group.name
    next
config application
    edit { id }
    # IDs of one or more applications that this shaper applies application control traffic shaping to.
        set id { integer }    Application IDs. range[0-4294967295]
    next
config app-category
    edit { id }
    # IDs of one or more application categories that this shaper applies application control traffic shaping to.
        set id { integer }    Category IDs. range[0-4294967295]
    next
config url-category
    edit { id }
    # IDs of one or more FortiGuard Web Filtering categories that this shaper applies traffic shaping to.
        set id { integer }    URL category ID. range[0-4294967295]
    next
config dstintf
    edit { name }
    # One or more outgoing (egress) interfaces.
        set name { string }    Interface name. size[64] - datasource(s): system.interface.name,system.zone.name
    next
    set traffic-shaper { string }    Traffic shaper to apply to traffic forwarded by the firewall policy. size[35] - datasource(s): fire-
wall.shaper.traffic-shaper.name
    set traffic-shaper-reverse { string }    Traffic shaper to apply to response traffic received by the firewall policy. size[35] - datasource
(s): firewall.shaper.traffic-shaper.name
    set per-ip-shaper { string }    Per-IP traffic shaper to apply with this policy. size[35] - datasource(s): firewall.shaper.per-ip-shaper.name
    next
end
```

firewall sniffer

Introduction.

```

config firewall sniffer
  edit { id }
  # Configure sniffer.
  set id { integer } Sniffer ID. range[0-9999]
  set status { enable | disable } Enable/disable the active status of the sniffer.
  set logtraffic { all | utm | disable } Either log all sessions, only sessions that have a security profile applied, or disable all logging
  for this policy.
    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.
  set ipv6 { enable | disable } Enable/disable sniffing IPv6 packets.
  set non-ip { enable | disable } Enable/disable sniffing non-IP packets.
  set interface { string } Interface name that traffic sniffing will take place on. size[35] - datasource(s): system.interface.name
  set host { string } 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). size[63]
  set port { string } Ports to sniff (Format examples: 10, :20, 30:40, 50-, 100-200). size[63]
  set protocol { string } Integer value for the protocol type as defined by IANA (0 - 255). size[63]
  set vlan { string } List of VLANs to sniff. size[63]
  set application-list-status { enable | disable } Enable/disable application control profile.
  set application-list { string } Name of an existing application list. size[35] - datasource(s): application.list.name
  set ips-sensor-status { enable | disable } Enable/disable IPS sensor.
  set ips-sensor { string } Name of an existing IPS sensor. size[35] - datasource(s): ips.sensor.name
  set dsri { enable | disable } Enable/disable DSRI.
  set av-profile-status { enable | disable } Enable/disable antivirus profile.
  set av-profile { string } Name of an existing antivirus profile. size[35] - datasource(s): antivirus.profile.name
  set webfilter-profile-status { enable | disable } Enable/disable web filter profile.
  set webfilter-profile { string } Name of an existing web filter profile. size[35] - datasource(s): webfilter.profile.name
  set spamfilter-profile-status { enable | disable } Enable/disable spam filter.
  set spamfilter-profile { string } Name of an existing spam filter profile. size[35] - datasource(s): spamfilter.profile.name
  set dlp-sensor-status { enable | disable } Enable/disable DLP sensor.
  set dlp-sensor { string } Name of an existing DLP sensor. size[35] - datasource(s): dlp.sensor.name
  set ips-dos-status { enable | disable } Enable/disable IPS DoS anomaly detection.
config anomaly
  edit { name }
  # Configuration method to edit Denial of Service (DoS) anomaly settings.

```

```

set name { string } Anomaly name. size[63]
set status { disable | enable } Enable/disable the active status of this anomaly sensor.
set log { enable | disable } Enable/disable logging for this anomaly.
set action { pass | block | proxy } Action taken when the threshold is reached.
    pass Allow traffic but record a log message if logging is enabled.
    block Block traffic if this anomaly is found.
    proxy Use a proxy to control the traffic flow.
set quarantine { none | attacker } Quarantine method.
    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.

```

    set quarantine-expiry { string } Duration of quarantine, from 1 minute to 364 days, 23 hours, and 59 minutes from now. (format:
###d##h##m, default = 5m). Requires quarantine set to attacker.
    set quarantine-log { disable | enable } Enable/disable quarantine logging.
    set threshold { integer } 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. range[1-2147483647]
    set threshold(default) { integer } Anomaly default threshold. range[0-4294967295]
next
set scan-botnet-connections { disable | block | monitor } Enable/disable scanning of connections to Botnet servers.
    disable Do not scan connections to botnet servers.
    block Block connections to botnet servers.
    monitor Log connections to botnet servers.
set max-packet-count { integer } Maximum packet count (1 - 1000000, default = 10000). range[1-1000000]
next
end

```

firewall ssl setting

Introduction.

```
config firewall ssl setting
    set proxy-connect-timeout { integer }    Time limit to make an internal connection to the appropriate proxy process (1 - 60 sec, default = 30).
    range[1-60]
    set ssl-dh-bits { 768 | 1024 | 1536 | 2048 }    Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).
        768    768-bit Diffie-Hellman prime.
        1024   1024-bit Diffie-Hellman prime.
        1536   1536-bit Diffie-Hellman prime.
        2048   2048-bit Diffie-Hellman prime.
    set ssl-send-empty-frags { enable | disable }    Enable/disable sending empty fragments to avoid attack on CBC IV (for SSL 3.0 and TLS 1.0 only).
    set no-matching-cipher-action { bypass | drop }    Bypass or drop the connection when no matching cipher is found.
        bypass Bypass connection.
        drop   Drop connection.
    set cert-cache-capacity { integer }    Maximum capacity of the host certificate cache (0 - 500, default = 200). range[0-500]
    set cert-cache-timeout { integer }    Time limit to keep certificate cache (1 - 120 min, default = 10). range[1-120]
    set session-cache-capacity { integer }    Capacity of the SSL session cache (--Obsolete--) (1 - 1000, default = 500). range[0-1000]
    set session-cache-timeout { integer }    Time limit to keep SSL session state (1 - 60 min, default = 20). range[1-60]
    set kxp-queue-threshold { integer }    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). range[0-512]
    set ssl-queue-threshold { integer }    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). range[0-512]
    set abbreviate-handshake { enable | disable }    Enable/disable use of SSL abbreviated handshake.
end
```

firewall ssl-server

Introduction.

```

config firewall ssl-server
  edit { name }
  # Configure SSL servers.
  set name { string }  Server name. size[35]
  set ip { ipv4 address any }  IPv4 address of the SSL server.
  set port { integer }  Server service port (1 - 65535, default = 443). range[1-65535]
  set ssl-mode { half | full }  SSL/TLS mode for encryption and decryption of traffic.
    half Client to FortiGate SSL.
    full Client to FortiGate and FortiGate to Server SSL.
  set add-header-x-forwarded-proto { enable | disable }  Enable/disable adding an X-Forwarded-Proto header to forwarded requests.
  set mapped-port { integer }  Mapped server service port (1 - 65535, default = 80). range[1-65535]
  set ssl-cert { string }  Name of certificate for SSL connections to this server (default = "Fortinet_CA_SSL"). size[35] - datasource(s):
  vpn.certificate.local.name
  set ssl-dh-bits { 768 | 1024 | 1536 | 2048 }  Bit-size of Diffie-Hellman (DH) prime used in DHE-RSA negotiation (default = 2048).
    768 768-bit Diffie-Hellman prime.
    1024 1024-bit Diffie-Hellman prime.
    1536 1536-bit Diffie-Hellman prime.
    2048 2048-bit Diffie-Hellman prime.
  set ssl-algorithm { high | medium | low }  Relative strength of encryption algorithms accepted in negotiation.
    high High encryption. Allow only AES and ChaCha
    medium Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
    low Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
  set ssl-client-renegotiation { allow | deny | secure }  Allow or block client renegotiation by server.
    allow Allow a SSL client to renegotiate.
    deny Abort any SSL connection that attempts to renegotiate.
    secure Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.
  set ssl-min-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  Lowest SSL/TLS version to negotiate.
    ssl-3.0 SSL 3.0.
    tls-1.0 TLS 1.0.
    tls-1.1 TLS 1.1.
    tls-1.2 TLS 1.2.
  set ssl-max-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  Highest SSL/TLS version to negotiate.
    ssl-3.0 SSL 3.0.
    tls-1.0 TLS 1.0.
    tls-1.1 TLS 1.1.

```

```
        tls-1.2 TLS 1.2.
    set ssl-send-empty-frags { enable | disable } Enable/disable sending empty fragments to avoid attack on CBC IV.
    set url-rewrite { enable | disable } Enable/disable rewriting the URL.
next
end
```


firewall ssl-ssh-profile

Introduction.

```
config firewall ssl-ssh-profile
edit { name }
# Configure SSL/SSH protocol options.
set name { string } Name. size[35]
set comment { string } Optional comments. size[255]
set inspect-all { disable | certificate-inspection | deep-inspection } Level of SSL inspection.
    disable Disable.
    certificate-inspection Inspect SSL handshake only.
    deep-inspection Full SSL inspection.
set client-cert-request { bypass | inspect | block } Action based on client certificate request failure.
    bypass Bypass.
    inspect Inspect.
    block Block.
set unsupported-ssl { bypass | inspect | block } Action based on the SSL encryption used being unsupported.
    bypass Bypass.
    inspect Inspect.
    block Block.
set allow-invalid-server-cert { enable | disable } When enabled, allows SSL sessions whose server certificate validation failed.
set untrusted-cert { allow | block | ignore } Allow, ignore, or block the untrusted SSL session server certificate.
    allow Allow the untrusted server certificate.
    block Block the connection when an untrusted server certificate is detected.
    ignore Always take the server certificate as trusted.
set ports { integer } Ports to use for scanning (1 - 65535, default = 443). range[1-65535]
set status { disable | certificate-inspection | deep-inspection } Configure protocol inspection status.
    disable Disable.
    certificate-inspection Inspect SSL handshake only.
    deep-inspection Full SSL inspection.
set client-cert-request { bypass | inspect | block } Action based on client certificate request failure.
    bypass Bypass.
    inspect Inspect.
    block Block.
set unsupported-ssl { bypass | inspect | block } Action based on the SSL encryption used being unsupported.
    bypass Bypass.
    inspect Inspect.
    block Block.
```

```
set allow-invalid-server-cert { enable | disable } When enabled, allows SSL sessions whose server certificate validation failed.
set untrusted-cert { allow | block | ignore } Allow, ignore, or block the untrusted SSL session server certificate.
    allow Allow the untrusted server certificate.
    block Block the connection when an untrusted server certificate is detected.
    ignore Always take the server certificate as trusted.
set ports { integer } Ports to use for scanning (1 - 65535, default = 443). range[1-65535]
set status { disable | deep-inspection } Configure protocol inspection status.
    disable Disable.
    deep-inspection Full SSL inspection.
set client-cert-request { bypass | inspect | block } Action based on client certificate request failure.
    bypass Bypass.
    inspect Inspect.
    block Block.
set unsupported-ssl { bypass | inspect | block } Action based on the SSL encryption used being unsupported.
    bypass Bypass.
    inspect Inspect.
    block Block.
set allow-invalid-server-cert { enable | disable } When enabled, allows SSL sessions whose server certificate validation failed.
set untrusted-cert { allow | block | ignore } Allow, ignore, or block the untrusted SSL session server certificate.
    allow Allow the untrusted server certificate.
    block Block the connection when an untrusted server certificate is detected.
    ignore Always take the server certificate as trusted.
set ports { integer } Ports to use for scanning (1 - 65535, default = 443). range[1-65535]
set status { disable | deep-inspection } Configure protocol inspection status.
    disable Disable.
    deep-inspection Full SSL inspection.
set client-cert-request { bypass | inspect | block } Action based on client certificate request failure.
    bypass Bypass.
    inspect Inspect.
    block Block.
set unsupported-ssl { bypass | inspect | block } Action based on the SSL encryption used being unsupported.
    bypass Bypass.
    inspect Inspect.
    block Block.
set allow-invalid-server-cert { enable | disable } When enabled, allows SSL sessions whose server certificate validation failed.
set untrusted-cert { allow | block | ignore } Allow, ignore, or block the untrusted SSL session server certificate.
    allow Allow the untrusted server certificate.
    block Block the connection when an untrusted server certificate is detected.
    ignore Always take the server certificate as trusted.
set ports { integer } Ports to use for scanning (1 - 65535, default = 443). range[1-65535]
set status { disable | deep-inspection } Configure protocol inspection status.
    disable Disable.
    deep-inspection Full SSL inspection.
```

```
set client-cert-request { bypass | inspect | block } Action based on client certificate request failure.
    bypass Bypass.
    inspect Inspect.
    block Block.
set unsupported-ssl { bypass | inspect | block } Action based on the SSL encryption used being unsupported.
    bypass Bypass.
    inspect Inspect.
    block Block.
set allow-invalid-server-cert { enable | disable } When enabled, allows SSL sessions whose server certificate validation failed.
set untrusted-cert { allow | block | ignore } Allow, ignore, or block the untrusted SSL session server certificate.
    allow Allow the untrusted server certificate.
    block Block the connection when an untrusted server certificate is detected.
    ignore Always take the server certificate as trusted.
set ports { integer } Ports to use for scanning (1 - 65535, default = 443). range[1-65535]
set status { disable | deep-inspection } Configure protocol inspection status.
    disable Disable.
    deep-inspection Full SSL inspection.
set client-cert-request { bypass | inspect | block } Action based on client certificate request failure.
    bypass Bypass.
    inspect Inspect.
    block Block.
set unsupported-ssl { bypass | inspect | block } Action based on the SSL encryption used being unsupported.
    bypass Bypass.
    inspect Inspect.
    block Block.
set allow-invalid-server-cert { enable | disable } When enabled, allows SSL sessions whose server certificate validation failed.
set untrusted-cert { allow | block | ignore } Allow, ignore, or block the untrusted SSL session server certificate.
    allow Allow the untrusted server certificate.
    block Block the connection when an untrusted server certificate is detected.
    ignore Always take the server certificate as trusted.
set ports { integer } Ports to use for scanning (1 - 65535, default = 443). range[1-65535]
set status { disable | deep-inspection } Configure protocol inspection status.
    disable Disable.
    deep-inspection Full SSL inspection.
set inspect-all { disable | deep-inspection } Level of SSL inspection.
    disable Disable.
    deep-inspection Full SSL inspection.
set block { x11-filter | ssh-shell | exec | port-forward } SSH blocking options.
    x11-filter X server forwarding
    ssh-shell SSH shell
    exec SSH execution
    port-forward Port forwarding
set log { x11-filter | ssh-shell | exec | port-forward } SSH logging options.
```

```

        x11-filter    X server forwarding
        ssh-shell     SSH shell
        exec          SSH execution
        port-forward  Port forwarding
set whitelist { enable | disable }  Enable/disable exempting servers by FortiGuard whitelist.
config ssl-exempt
  edit { id }
  # Servers to exempt from SSL inspection.
  set id { integer }  ID number. range[0-255]
  set type { fortiguard-category | address | address6 }  Type of address object (IPv4 or IPv6) or FortiGuard category.
    fortiguard-category  FortiGuard category.
    address              Firewall IPv4 address.
    address6             Firewall IPv6 address.
  set fortiguard-category { integer }  FortiGuard category ID. range[0-255]
  set address { string }  IPv4 address object. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
  set address6 { string }  IPv6 address object. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
set server-cert-mode { re-sign | replace }  Re-sign or replace the server's certificate.
  re-sign  Multiple clients connecting to multiple servers.
  replace  Protect an SSL server.
set use-ssl-server { disable | enable }  Enable/disable the use of SSL server table for SSL offloading.
set caname { string }  CA certificate used by SSL Inspection. size[35] - datasource(s): vpn.certificate.local.name
set untrusted-caname { string }  Untrusted CA certificate used by SSL Inspection. size[35] - datasource(s): vpn.certificate.local.name
set server-cert { string }  Certificate used by SSL Inspection to replace server certificate. size[35] - datasource(s): vpn.cer-
tificate.local.name
config ssl-server
  edit { id }
  # SSL servers.
  set id { integer }  SSL server ID. range[0-4294967295]
  set ip { ipv4 address any }  IPv4 address of the SSL server.
  set https-client-cert-request { bypass | inspect | block }  Action based on client certificate request failure during the HTTPS hand-
shake.
    bypass  Bypass.
    inspect  Inspect.
    block  Block.
  set smtps-client-cert-request { bypass | inspect | block }  Action based on client certificate request failure during the SMTPS hand-
shake.
    bypass  Bypass.
    inspect  Inspect.
    block  Block.
  set pop3s-client-cert-request { bypass | inspect | block }  Action based on client certificate request failure during the POP3S hand-
shake.
    bypass  Bypass.

```

```
        inspect Inspect.
        block Block.
    set imaps-client-cert-request { bypass | inspect | block } Action based on client certificate request failure during the IMAPS handshake.
        bypass Bypass.
        inspect Inspect.
        block Block.
    set ftps-client-cert-request { bypass | inspect | block } Action based on client certificate request failure during the FTPS handshake.
        bypass Bypass.
        inspect Inspect.
        block Block.
    set ssl-other-client-cert-request { bypass | inspect | block } Action based on client certificate request failure during an SSL protocol handshake.
        bypass Bypass.
        inspect Inspect.
        block Block.
    next
    set ssl-anomalies-log { disable | enable } Enable/disable logging SSL anomalies.
    set ssl-exemptions-log { disable | enable } Enable/disable logging SSL exemptions.
    set rpc-over-https { enable | disable } Enable/disable inspection of RPC over HTTPS.
    set mapi-over-https { enable | disable } Enable/disable inspection of MAPI over HTTPS.
    next
end
```

firewall ttl-policy

Introduction.

```
config firewall ttl-policy
  edit { id }
  # Configure TTL policies.
  set id { integer } ID. range[0-4294967295]
  set status { enable | disable } Enable/disable this TTL policy.
  set action { accept | deny } Action to be performed on traffic matching this policy (default = deny).
    accept Allow traffic matching this policy.
    deny Deny or block traffic matching this policy.
  set srcintf { string } Source interface name from available interfaces. size[35] - datasource(s): system.zone.name,system.interface.name
  config srcaddr
    edit { name }
    # Source address object(s) from available options. Separate multiple names with a space.
    set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config service
    edit { name }
    # Service object(s) from available options. Separate multiple names with a space.
    set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
  set schedule { string } Schedule object from available options. size[35] - datasource(s): fire-
wall.schedule.onetime.name,firewall.schedule.recurring.name,firewall.schedule.group.name
  set ttl { string } Value/range to match against the packet's Time to Live value (format: ttl[ - ttl_high], 1 - 255).
  next
end
```

firewall {vip | vip6}

Configure firewall virtual IPs (VIPs) and their associated addresses and port mappings (NAT). Use VIPs to configure destination NAT and server load balancing. For information about FortiOS Firewall VIPs in general, see [Virtual IPs](#). For information about server load balancing with FortiOS Firewall VIPs see [Server Load Balancing](#).

```
config firewall vip
  edit { name }
  # Configure virtual IP for IPv4.
  set name { string }   Virtual IP name. size[63]
  set id { integer }    Custom defined ID. range[0-65535]
  set uuid { uuid }     Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set comment { string } Comment. size[255]
  set type { option }   Configure a static NAT, load balance, server load balance, DNS translation, or FQDN VIP.
    static-nat          Static NAT.
    load-balance         Load balance.
    server-load-balance Server load balance.
    dns-translation     DNS translation.
    fqdn                 Fully qualified domain name.
  set dns-mapping-ttl { integer } DNS mapping TTL (Set to zero to use TTL in DNS response, default = 0). range[0-604800]
  set ldb-method { option } Method used to distribute sessions to real servers.
    static               Distribute to server based on source IP.
    round-robin          Distribute to server based round robin order.
    weighted             Distribute to server based on weight.
    least-session        Distribute to server with lowest session count.
    least-rtt            Distribute to server with lowest Round-Trip-Time.
    first-alive          Distribute to the first server that is alive.
    http-host            Distribute to server based on host field in HTTP header.
  config src-filter
    edit { 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.
      set range { string } Source-filter range. size[64]
    next
  config service
    edit { name }
    # Service name.
      set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name, firewall.service.group.name
```

```

    next
    set extip { string } IP address or address range on the external interface that you want to map to an address or address range on the destination network.
    config extaddr
        edit { name }
            # External FQDN address name.
            set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
        next
    config mappedip
        edit { range }
            # IP address or address range on the destination network to which the external IP address is mapped.
            set range { string } Mapped IP range. size[64]
        next
    set mapped-addr { string } Mapped FQDN address name. size[63] - datasource(s): firewall.address.name
    set extintf { string } Interface connected to the source network that receives the packets that will be forwarded to the destination network. size[35] - datasource(s): system.interface.name
    set arp-reply { disable | enable } Enable to respond to ARP requests for this virtual IP address. Enabled by default.
    set server-type { option } Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).
        http HTTP
        https HTTPS
        imaps IMAPS
        pop3s POP3S
        smtps SMTPS
        ssl SSL
        tcp TCP
        udp UDP
        ip IP
    set persistence { none | http-cookie | ssl-session-id } 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.
        none None.
        http-cookie HTTP cookie.
        ssl-session-id SSL session ID.
    set nat-source-vip { disable | enable } Enable to prevent unintended servers from using a virtual IP. Disable to use the actual IP address of the server as the source address.
    set portforward { disable | enable } Enable/disable port forwarding.
    set protocol { tcp | udp | sctp | icmp } Protocol to use when forwarding packets.
        tcp TCP.
        udp UDP.
        sctp SCTP.
        icmp ICMP.
    set extport { string } Incoming port number range that you want to map to a port number range on the destination network.
    set mappedport { string } Port number range on the destination network to which the external port number range is mapped.
    set gratuitous-arp-interval { integer } Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to

```



```

enable. range[5-8640000]
config srcintf-filter
    edit { interface-name }
        # Interfaces to which the VIP applies. Separate the names with spaces.
        set interface-name { string }    Interface name. size[64] - datasource(s): system.interface.name
    next
set portmapping-type { 1-to-1 | m-to-n }    Port mapping type.
    1-to-1    One to one.
    m-to-n    Many to many.
config realservers
    edit { id }
        # Select the real servers that this server load balancing VIP will distribute traffic to.
        set id { integer }    Real server ID. range[0-4294967295]
        set ip { ipv4 address any }    IP address of the real server.
        set port { integer }    Port for communicating with the real server. Required if port forwarding is enabled. range[1-65535]
        set status { active | standby | disable }    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.
            active    Server status active.
            standby    Server status standby.
            disable    Server status disable.
        set weight { integer }    Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets
more connections. range[1-255]
        set holddown-interval { integer }    Time in seconds that the health check monitor continues to monitor and unresponsive server that
should be active. range[30-65535]
        set healthcheck { disable | enable | vip }    Enable to check the responsiveness of the real server before forwarding traffic.
        set http-host { string }    HTTP server domain name in HTTP header. size[63]
        set max-connections { integer }    Max number of active connections that can be directed to the real server. When reached, sessions
are sent to other real servers. range[0-2147483647]
        set monitor { string }    Name of the health check monitor to use when polling to determine a virtual server's connectivity status.
size[64] - datasource(s): firewall.ldb-monitor.name
        set client-ip { string }    Only clients in this IP range can connect to this real server.
    next
set http-cookie-domain-from-host { disable | enable }    Enable/disable use of HTTP cookie domain from host field in HTTP.
set http-cookie-domain { string }    Domain that HTTP cookie persistence should apply to. size[35]
set http-cookie-path { string }    Limit HTTP cookie persistence to the specified path. size[35]
set http-cookie-generation { integer }    Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies. range[0-
4294967295]
set http-cookie-age { integer }    Time in minutes that client web browsers should keep a cookie. Default is 60 seconds. 0 = no time limit.
range[0-525600]
set http-cookie-share { disable | same-ip }    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.
    disable    Only allow HTTP cookie to match this virtual server.
    same-ip    Allow HTTP cookie to match any virtual server with same IP.

```

```

set https-cookie-secure { disable | enable } Enable/disable verification that inserted HTTPS cookies are secure.
set http-multiplex { enable | disable } Enable/disable HTTP multiplexing.
set http-ip-header { enable | disable } For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP
header.
set http-ip-header-name { string } 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. size[35]
set outlook-web-access { disable | enable } Enable to add the Front-End-Https header for Microsoft Outlook Web Access.
set weblogic-server { disable | enable } Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.
set websphere-server { disable | enable } Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.
set ssl-mode { half | full } 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).
    half Client to FortiGate SSL.
    full Client to FortiGate and FortiGate to Server SSL.
set ssl-certificate { string } The name of the SSL certificate to use for SSL acceleration. size[35] - datasource(s): vpn.cer-
tificate.local.name
set ssl-dh-bits { option } Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.
    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.
set ssl-algorithm { high | medium | low | custom } Permitted encryption algorithms for SSL sessions according to encryption strength.
    high High encryption. Allow only AES and ChaCha.
    medium Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
    low Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
    custom Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.
config ssl-cipher-suites
edit { priority }
# SSL/TLS cipher suites acceptable from a client, ordered by priority.
set priority { integer } SSL/TLS cipher suites priority. range[0-4294967295]
set cipher { option } Cipher suite name.
    TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256 Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
    TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256 Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
    TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256 Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
    TLS-DHE-RSA-WITH-AES-128-CBC-SHA Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
    TLS-DHE-RSA-WITH-AES-256-CBC-SHA Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
    TLS-DHE-RSA-WITH-AES-128-CBC-SHA256 Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
    TLS-DHE-RSA-WITH-AES-128-GCM-SHA256 Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
    TLS-DHE-RSA-WITH-AES-256-CBC-SHA256 Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
    TLS-DHE-RSA-WITH-AES-256-GCM-SHA384 Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
    TLS-DHE-DSS-WITH-AES-128-CBC-SHA Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.
    TLS-DHE-DSS-WITH-AES-256-CBC-SHA Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.

```

TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA.
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA.
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA256.
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-GCM-SHA256.
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-SEED-CBC-SHA.
TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-SEED-CBC-SHA.
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.
TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite	TLS-RSA-WITH-SEED-CBC-SHA.
TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-ARIA-128-CBC-SHA256.
TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-RSA-WITH-ARIA-256-CBC-SHA384.

```

        TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256      Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.
        TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384      Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.
        TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256    Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.
        TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384    Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.
        TLS-ECDHE-RSA-WITH-RC4-128-SHA              Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
        TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA         Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
        TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA           Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
        TLS-RSA-WITH-3DES-EDE-CBC-SHA                Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
        TLS-RSA-WITH-RC4-128-MD5                     Cipher suite TLS-RSA-WITH-RC4-128-MD5.
        TLS-RSA-WITH-RC4-128-SHA                     Cipher suite TLS-RSA-WITH-RC4-128-SHA.
        TLS-DHE-RSA-WITH-DES-CBC-SHA                 Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.
        TLS-DHE-DSS-WITH-DES-CBC-SHA                 Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.
        TLS-RSA-WITH-DES-CBC-SHA                     Cipher suite TLS-RSA-WITH-DES-CBC-SHA.
set versions { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  SSL/TLS versions that the cipher suite can be used with.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.

next
set ssl-server-algorithm { option }  Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption
strength.
    high    High encryption. Allow only AES and ChaCha.
    medium  Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
    low     Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
    custom  Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.
    client  Use the same encryption algorithms for both client and server sessions.

config ssl-server-cipher-suites
edit { priority }
# SSL/TLS cipher suites to offer to a server, ordered by priority.
set priority { integer }  SSL/TLS cipher suites priority. range[0-4294967295]
set cipher { option }  Cipher suite name.
    TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256      Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
    TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256    Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
    TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256        Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
    TLS-DHE-RSA-WITH-AES-128-CBC-SHA                 Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
    TLS-DHE-RSA-WITH-AES-256-CBC-SHA                 Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
    TLS-DHE-RSA-WITH-AES-128-CBC-SHA256             Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
    TLS-DHE-RSA-WITH-AES-128-GCM-SHA256             Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
    TLS-DHE-RSA-WITH-AES-256-CBC-SHA256             Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
    TLS-DHE-RSA-WITH-AES-256-GCM-SHA384             Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
    TLS-DHE-DSS-WITH-AES-128-CBC-SHA                 Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.
    TLS-DHE-DSS-WITH-AES-256-CBC-SHA                 Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
    TLS-DHE-DSS-WITH-AES-128-CBC-SHA256             Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.

```

TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA.
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA.
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA256.
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-GCM-SHA256.
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-SEED-CBC-SHA.
TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-SEED-CBC-SHA.
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.
TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite	TLS-RSA-WITH-SEED-CBC-SHA.
TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-ARIA-128-CBC-SHA256.
TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-RSA-WITH-ARIA-256-CBC-SHA384.
TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.

```

    TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384      Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.
    TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256    Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.
    TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384    Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.
    TLS-ECDHE-RSA-WITH-RC4-128-SHA              Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
    TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA        Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
    TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA          Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
    TLS-RSA-WITH-3DES-EDE-CBC-SHA              Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
    TLS-RSA-WITH-RC4-128-MD5                   Cipher suite TLS-RSA-WITH-RC4-128-MD5.
    TLS-RSA-WITH-RC4-128-SHA                   Cipher suite TLS-RSA-WITH-RC4-128-SHA.
    TLS-DHE-RSA-WITH-DES-CBC-SHA                Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.
    TLS-DHE-DSS-WITH-DES-CBC-SHA                Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.
    TLS-RSA-WITH-DES-CBC-SHA                    Cipher suite TLS-RSA-WITH-DES-CBC-SHA.
set versions { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  SSL/TLS versions that the cipher suite can be used with.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.

```

next

set ssl-pfs { require | deny | allow } Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.

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.

set ssl-min-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 } Lowest SSL/TLS version acceptable from a client.

ssl-3.0 SSL 3.0.

tls-1.0 TLS 1.0.

tls-1.1 TLS 1.1.

tls-1.2 TLS 1.2.

set ssl-max-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 } Highest SSL/TLS version acceptable from a client.

ssl-3.0 SSL 3.0.

tls-1.0 TLS 1.0.

tls-1.1 TLS 1.1.

tls-1.2 TLS 1.2.

set ssl-server-min-version { option } Lowest SSL/TLS version acceptable from a server. Use the client setting by default.

ssl-3.0 SSL 3.0.

tls-1.0 TLS 1.0.

tls-1.1 TLS 1.1.

tls-1.2 TLS 1.2.

client Use same value as client configuration.

set ssl-server-max-version { option } Highest SSL/TLS version acceptable from a server. Use the client setting by default.

ssl-3.0 SSL 3.0.

tls-1.0 TLS 1.0.

tls-1.1 TLS 1.1.

```

        tls-1.2 TLS 1.2.
        client Use same value as client configuration.
        set ssl-send-empty-frags { enable | disable } 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.
        set ssl-client-fallback { disable | enable } Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).
        set ssl-client-renegotiation { allow | deny | secure } Allow, deny, or require secure renegotiation of client sessions to comply with RFC
5746.
                allow Allow a SSL client to renegotiate.
                deny Abort any client initiated SSL re-negotiation attempt.
                secure Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.
        set ssl-client-session-state-type { disable | time | count | both } How to expire SSL sessions for the segment of the SSL connection
between the client and the FortiGate.
                disable Do not keep session states.
                time Expire session states after this many minutes.
                count Expire session states when this maximum is reached.
                both Expire session states based on time or count, whichever occurs first.
        set ssl-client-session-state-timeout { integer } Number of minutes to keep client to FortiGate SSL session state. range[1-14400]
        set ssl-client-session-state-max { integer } Maximum number of client to FortiGate SSL session states to keep. range[1-10000]
        set ssl-server-session-state-type { disable | time | count | both } How to expire SSL sessions for the segment of the SSL connection
between the server and the FortiGate.
                disable Do not keep session states.
                time Expire session states after this many minutes.
                count Expire session states when this maximum is reached.
                both Expire session states based on time or count, whichever occurs first.
        set ssl-server-session-state-timeout { integer } Number of minutes to keep FortiGate to Server SSL session state. range[1-14400]
        set ssl-server-session-state-max { integer } Maximum number of FortiGate to Server SSL session states to keep. range[1-10000]
        set ssl-http-location-conversion { enable | disable } Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.
        set ssl-http-match-host { enable | disable } Enable/disable HTTP host matching for location conversion.
        set ssl-hpkp { disable | enable | report-only } Enable/disable including HPKP header in response.
        set ssl-hpkp-primary { string } Certificate to generate primary HPKP pin from. size[35] - datasource(s): vpn.cer-
tificate.local.name,vpn.certificate.ca.name
        set ssl-hpkp-backup { string } Certificate to generate backup HPKP pin from. size[35] - datasource(s):
vpn.certificate.local.name,vpn.certificate.ca.name
        set ssl-hpkp-age { integer } Number of seconds the client should honour the HPKP setting. range[60-157680000]
        set ssl-hpkp-report-uri { string } URL to report HPKP violations to. size[255]
        set ssl-hpkp-include-subdomains { disable | enable } Indicate that HPKP header applies to all subdomains.
        set ssl-hsts { disable | enable } Enable/disable including HSTS header in response.
        set ssl-hsts-age { integer } Number of seconds the client should honour the HSTS setting. range[60-157680000]
        set ssl-hsts-include-subdomains { disable | enable } Indicate that HSTS header applies to all subdomains.
config monitor
    edit { name }
        # Name of the health check monitor to use when polling to determine a virtual server's connectivity status.
        set name { string } Health monitor name. size[64] - datasource(s): firewall.ldb-monitor.name

```

```
        next
        set max-embryonic-connections { integer } Maximum number of incomplete connections. range[0-100000]
        set color { integer } Color of icon on the GUI. range[0-32]
    next
end

config firewall vip6
edit { name }
# Configure virtual IP for IPv6.
set name { string } Virtual ip6 name. size[63]
set id { integer } Custom defined ID. range[0-65535]
set uuid { uuid } Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
set comment { string } Comment. size[255]
set type { static-nat | server-load-balance } Configure a static NAT or server load balance VIP.
    static-nat Static NAT.
    server-load-balance Server load balance.
config src-filter
edit { range }
# Source IP6 filter (x::x::x::x::x::x/x). Separate addresses with spaces.
set range { string } Source-filter range. size[79]
next
set extip { string } IP address or address range on the external interface that you want to map to an address or address range on the destination network.
set mappedip { string } Mapped IP address range in the format startIP-endIP.
set arp-reply { disable | enable } Enable to respond to ARP requests for this virtual IP address. Enabled by default.
set portforward { disable | enable } Enable port forwarding.
set protocol { tcp | udp | sctp } Protocol to use when forwarding packets.
    tcp TCP.
    udp UDP.
    sctp SCTP.
set extport { string } Incoming port number range that you want to map to a port number range on the destination network.
set mappedport { string } Port number range on the destination network to which the external port number range is mapped.
set color { integer } Color of icon on the GUI. range[0-32]
set ldb-method { option } Method used to distribute sessions to real servers.
    static Distribute sessions based on source IP.
    round-robin Distribute sessions based round robin order.
    weighted Distribute sessions based on weight.
    least-session Sends new sessions to the server with the lowest session count.
    least-rtt Distribute new sessions to the server with lowest Round-Trip-Time.
    first-alive Distribute sessions to the first server that is alive.
    http-host Distribute sessions to servers based on host field in HTTP header.
set server-type { option } Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).
```



```

    http    HTTP
    https   HTTPS
    imaps   IMAPS
    pop3s   POP3S
    smtps   SMTPS
    ssl     SSL
    tcp     TCP
    udp     UDP
    ip      IP

    set persistence { none | http-cookie | ssl-session-id }  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.
        none          None.
        http-cookie    HTTP cookie.
        ssl-session-id SSL session ID.
config realservers
    edit { id }
        # Select the real servers that this server load balancing VIP will distribute traffic to.
        set id { integer }  Real server ID. range[0-4294967295]
        set ip { ipv6 prefix }  IPv6 address of the real server.
        set port { integer }  Port for communicating with the real server. Required if port forwarding is enabled. range[1-65535]
        set status { active | standby | disable }  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.
            active    Server status active.
            standby   Server status standby.
            disable   Server status disable.

        set weight { integer }  Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets
more connections. range[1-255]
        set holddown-interval { integer }  Time in seconds that the health check monitor continues to monitor an unresponsive server that
should be active. range[30-65535]
        set healthcheck { disable | enable | vip }  Enable to check the responsiveness of the real server before forwarding traffic.
        set http-host { string }  HTTP server domain name in HTTP header. size[63]
        set max-connections { integer }  Max number of active connections that can directed to the real server. When reached, sessions are
sent to other real servers. range[0-2147483647]
        set monitor { string }  Name of the health check monitor to use when polling to determine a virtual server's connectivity status.
size[64] - datasource(s): firewall.ldb-monitor.name
        set client-ip { string }  Only clients in this IP range can connect to this real server.
    next
    set http-cookie-domain-from-host { disable | enable }  Enable/disable use of HTTP cookie domain from host field in HTTP.
    set http-cookie-domain { string }  Domain that HTTP cookie persistence should apply to. size[35]
    set http-cookie-path { string }  Limit HTTP cookie persistence to the specified path. size[35]
    set http-cookie-generation { integer }  Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies. range[0-
4294967295]
    set http-cookie-age { integer }  Time in minutes that client web browsers should keep a cookie. Default is 60 seconds. 0 = no time limit.

```

```

range[0-525600]
    set http-cookie-share { disable | same-ip } 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.
        disable Only allow HTTP cookie to match this virtual server.
        same-ip Allow HTTP cookie to match any virtual server with same IP.
    set https-cookie-secure { disable | enable } Enable/disable verification that inserted HTTPS cookies are secure.
    set http-multiplex { enable | disable } Enable/disable HTTP multiplexing.
    set http-ip-header { enable | disable } For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP
header.
    set http-ip-header-name { string } 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. size[35]
    set outlook-web-access { disable | enable } Enable to add the Front-End-Https header for Microsoft Outlook Web Access.
    set weblogic-server { disable | enable } Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.
    set websphere-server { disable | enable } Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.
    set ssl-mode { half | full } 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).
        half Client to FortiGate SSL.
        full Client to FortiGate and FortiGate to Server SSL.
    set ssl-certificate { string } The name of the SSL certificate to use for SSL acceleration. size[35] - datasource(s): vpn.cer-
tificate.local.name
    set ssl-dh-bits { option } Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.
        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.
    set ssl-algorithm { high | medium | low | custom } Permitted encryption algorithms for SSL sessions according to encryption strength.
        high Use AES or 3DES.
        medium Use AES, 3DES, or RC4.
        low Use AES, 3DES, RC4, or DES.
        custom Use config ssl-cipher-suites to select the cipher suites that are allowed.
config ssl-cipher-suites
    edit { priority }
    # SSL/TLS cipher suites acceptable from a client, ordered by priority.
    set priority { integer } SSL/TLS cipher suites priority. range[0-4294967295]
    set cipher { option } Cipher suite name.
        TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256 Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
        TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256 Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
        TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256 Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
        TLS-DHE-RSA-WITH-AES-128-CBC-SHA Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
        TLS-DHE-RSA-WITH-AES-256-CBC-SHA Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
        TLS-DHE-RSA-WITH-AES-128-CBC-SHA256 Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.

```

TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-AES-128-CBC-SHA.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA.
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA.
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA256.
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-GCM-SHA256.
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-SEED-CBC-SHA.
TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-SEED-CBC-SHA.
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.

```

        TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256      Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.
        TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384      Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.
        TLS-RSA-WITH-SEED-CBC-SHA                  Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.
        TLS-RSA-WITH-ARIA-128-CBC-SHA256          Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.
        TLS-RSA-WITH-ARIA-256-CBC-SHA384          Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.
        TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256    Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.
        TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384    Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.
        TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256  Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.
        TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384  Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.
        TLS-ECDHE-RSA-WITH-RC4-128-SHA            Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
        TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA       Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
        TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA         Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
        TLS-RSA-WITH-3DES-EDE-CBC-SHA             Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
        TLS-RSA-WITH-RC4-128-MD5                  Cipher suite TLS-RSA-WITH-RC4-128-MD5.
        TLS-RSA-WITH-RC4-128-SHA                  Cipher suite TLS-RSA-WITH-RC4-128-SHA.
        TLS-DHE-RSA-WITH-DES-CBC-SHA              Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.
        TLS-DHE-DSS-WITH-DES-CBC-SHA             Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.
        TLS-RSA-WITH-DES-CBC-SHA                  Cipher suite TLS-RSA-WITH-DES-CBC-SHA.
    set versions { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  SSL/TLS versions that the cipher suite can be used with.
        ssl-3.0  SSL 3.0.
        tls-1.0  TLS 1.0.
        tls-1.1  TLS 1.1.
        tls-1.2  TLS 1.2.
    next
    set ssl-server-algorithm { option }  Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption
strength.
        high  Use AES or 3DES.
        medium  Use AES, 3DES, or RC4.
        low  Use AES, 3DES, RC4, or DES.
        custom  Use config ssl-server-cipher-suites to select the cipher suites that are allowed.
        client  Use the same encryption algorithms for client and server sessions.
    config ssl-server-cipher-suites
        edit { priority }
        # SSL/TLS cipher suites to offer to a server, ordered by priority.
        set priority { integer }  SSL/TLS cipher suites priority. range[0-4294967295]
        set cipher { option }  Cipher suite name.
            TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256  Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
            TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256  Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
            TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256  Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
            TLS-DHE-RSA-WITH-AES-128-CBC-SHA  Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
            TLS-DHE-RSA-WITH-AES-256-CBC-SHA  Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
            TLS-DHE-RSA-WITH-AES-128-CBC-SHA256  Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.
            TLS-DHE-RSA-WITH-AES-128-GCM-SHA256  Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.

```

TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-AES-128-CBC-SHA.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-AES-256-CBC-SHA.
TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.
TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.
TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.
TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA.
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA.
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-CBC-SHA256.
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite	TLS-RSA-WITH-AES-128-GCM-SHA256.
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-AES-256-CBC-SHA256.
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite	TLS-RSA-WITH-AES-256-GCM-SHA384.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite	TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.
TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-RSA-WITH-SEED-CBC-SHA.
TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite	TLS-DHE-DSS-WITH-SEED-CBC-SHA.
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.

```

    TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384      Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.
    TLS-RSA-WITH-SEED-CBC-SHA                  Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.
    TLS-RSA-WITH-ARIA-128-CBC-SHA256          Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.
    TLS-RSA-WITH-ARIA-256-CBC-SHA384          Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.
    TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256    Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.
    TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384    Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.
    TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256  Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.
    TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384  Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.
    TLS-ECDHE-RSA-WITH-RC4-128-SHA            Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.
    TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA       Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.
    TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA         Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.
    TLS-RSA-WITH-3DES-EDE-CBC-SHA             Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.
    TLS-RSA-WITH-RC4-128-MD5                  Cipher suite TLS-RSA-WITH-RC4-128-MD5.
    TLS-RSA-WITH-RC4-128-SHA                  Cipher suite TLS-RSA-WITH-RC4-128-SHA.
    TLS-DHE-RSA-WITH-DES-CBC-SHA              Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.
    TLS-DHE-DSS-WITH-DES-CBC-SHA              Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.
    TLS-RSA-WITH-DES-CBC-SHA                  Cipher suite TLS-RSA-WITH-DES-CBC-SHA.
set versions { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  SSL/TLS versions that the cipher suite can be used with.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.

next
set ssl-pfs { require | deny | allow }  Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.
    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.
set ssl-min-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  Lowest SSL/TLS version acceptable from a client.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.
set ssl-max-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 }  Highest SSL/TLS version acceptable from a client.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.
set ssl-server-min-version { option }  Lowest SSL/TLS version acceptable from a server. Use the client setting by default.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.

```

```

    client    Use same value as client configuration.
set ssl-server-max-version { option }    Highest SSL/TLS version acceptable from a server. Use the client setting by default.
    ssl-3.0  SSL 3.0.
    tls-1.0  TLS 1.0.
    tls-1.1  TLS 1.1.
    tls-1.2  TLS 1.2.
    client    Use same value as client configuration.
set ssl-send-empty-frags { enable | disable }    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.
set ssl-client-fallback { disable | enable }    Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).
set ssl-client-renegotiation { allow | deny | secure }    Allow, deny, or require secure renegotiation of client sessions to comply with RFC
5746.
    allow    Allow a SSL client to renegotiate.
    deny     Abort any SSL connection that attempts to renegotiate.
    secure   Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.
set ssl-client-session-state-type { disable | time | count | both }    How to expire SSL sessions for the segment of the SSL connection
between the client and the FortiGate.
    disable  Do not keep session states.
    time     Expire session states after this many minutes.
    count    Expire session states when this maximum is reached.
    both     Expire session states based on time or count, whichever occurs first.
set ssl-client-session-state-timeout { integer }    Number of minutes to keep client to FortiGate SSL session state. range[1-14400]
set ssl-client-session-state-max { integer }    Maximum number of client to FortiGate SSL session states to keep. range[1-10000]
set ssl-server-session-state-type { disable | time | count | both }    How to expire SSL sessions for the segment of the SSL connection
between the server and the FortiGate.
    disable  Do not keep session states.
    time     Expire session states after this many minutes.
    count    Expire session states when this maximum is reached.
    both     Expire session states based on time or count, whichever occurs first.
set ssl-server-session-state-timeout { integer }    Number of minutes to keep FortiGate to Server SSL session state. range[1-14400]
set ssl-server-session-state-max { integer }    Maximum number of FortiGate to Server SSL session states to keep. range[1-10000]
set ssl-http-location-conversion { enable | disable }    Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.
set ssl-http-match-host { enable | disable }    Enable/disable HTTP host matching for location conversion.
set ssl-hpkp { disable | enable | report-only }    Enable/disable including HPKP header in response.
set ssl-hpkp-primary { string }    Certificate to generate primary HPKP pin from. size[35] - datasource(s): vpn.cer-
tificate.local.name, vpn.certificate.ca.name
set ssl-hpkp-backup { string }    Certificate to generate backup HPKP pin from. size[35] - datasource(s):
vpn.certificate.local.name, vpn.certificate.ca.name
set ssl-hpkp-age { integer }    Number of minutes the web browser should keep HPKP. range[60-157680000]
set ssl-hpkp-report-uri { string }    URL to report HPKP violations to. size[255]
set ssl-hpkp-include-subdomains { disable | enable }    Indicate that HPKP header applies to all subdomains.
set ssl-hsts { disable | enable }    Enable/disable including HSTS header in response.
set ssl-hsts-age { integer }    Number of seconds the client should honour the HSTS setting. range[60-157680000]

```

```
set ssl-hsts-include-subdomains { disable | enable }  Indicate that HSTS header applies to all subdomains.
config monitor
  edit { name }
    # Name of the health check monitor to use when polling to determine a virtual server's connectivity status.
    set name { string }  Health monitor name. size[64] - datasource(s): firewall.ldb-monitor.name
  next
set max-embryonic-connections { integer }  Maximum number of incomplete connections. range[0-100000]
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

uuid

Each VIP has a Universally Unique Identifier (UUID) that is automatically assigned. It is a 128 bit value written in hexadecimal. It can be edited.

comment <comment>

Add a comment about the VIP.

type {dns-translation | load-balance | server-load-balance | static-nat}

Select the type of static or dynamic NAT applied by the virtual IP.

- `dns-translation` dynamic VIP with DNS translation.
- `load-balance` dynamic NAT load balancing with server selection from an IP address range.
- `server-load-balance` dynamic NAT load balancing with server selection from among up to eight realservers, determined by your selected load balancing algorithm and server responsiveness monitors. Includes SSL offloading.
- `static-nat` Static NAT (the default).
- `fqdn` dynamic fully qualified domain name (FQDN) VIP.

ldb-method {first-alive | http-host | least-rtt | least-session | round-robin | static | weighted}

Select the method used by the virtual server to distribute sessions to the real servers. You add real servers to the virtual server using `configrealservers`.

This option appears only if `type` is `server-loadbalance`.

`first-alive` Always directs requests to the first alive real server. In this case “first” refers to the order of the real servers in the virtual server configuration. For example, if you add real servers A, B and C in that order, then traffic always goes to A as long as it is alive. If A goes down then traffic goes to B and if B goes down the traffic goes to C. If A comes back up, traffic goes to A. Real servers are ordered in the virtual server configuration in the order in which you add them, with the most recently added real server last. If you want to change the order you must delete and re-add real servers as required.

`http-host` Load balance HTTP requests by the contents of the HOST header.

`least-rtt` Directs requests to the real server with the least round trip time. The round trip time is determined by a Ping monitor and is defaulted to 0 if no Ping monitors are defined.

`least-session` Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing have similar capabilities.

`round-robin` Directs request to the next real server, and treats all real servers as equals regardless of response time or number of connections. Unresponsive real servers are avoided. A separate real server is required.

`static` (the default) Distributes sessions evenly across all real servers according to the session source IP address. This load balancing method provides some persistence because all sessions from the same source address would always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not required. (the default) Distributes sessions evenly across all real servers according to the session source IP address. This load balancing method provides some persistence because all sessions from the same source address would always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not required.

`weighted` Real servers with a higher weight value receive a larger percentage of connections at any one time. Server weights can be set in `config realservers set weight`.

dns-mapping-ttl

Enter time-to-live for DNS response. Range 0 to 604 800. Available when `type` is `dns-translation`. Default is 0 which means use the DNS server's response time.

src-filter <address> [<address>...]

Enter a 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). Separate addresses by spaces.

extip <address>[-<address>]

Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network. If `type` is `static-nat` and `mappedip` is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. To configure a dynamic virtual IP that accepts connections destined for any IP address, set `extip` to 0.0.0.0.

mappedip <address> [<address>...]

Enter the IP address or IP address range on the destination network to which the external IP address is mapped. If `type` is `static-nat` and `mappedip` is an IP address range, FortiOS uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. If `type` is `load-balance` and `mappedip` is an IP address range, the FortiGate unit uses `extip` as a single IP address to create a one-to-many mapping. Input each address (separated by spaces) in the format of IP (x.x.x.x), IP subnet (x.x.x.x/y) or IP range (x.x.x.x-y.y.y.y).

extintf <name>

Enter the name of the interface connected to the source network that receives the packets that will be forwarded to the destination network. The interface name can be any FortiGate network interface, VLAN subinterface, IPSec VPN interface, or modem interface.

arp-reply {disable | enable}

Enable to respond to ARP requests for this virtual IP address. Enabled by default.

server-type {http | https | imaps | ip | pop3s | smtps | ssl | tcp | udp}

If the `type` is `server-load-balance`, select the protocol to be load balanced by the virtual server (also called the server load balance virtual IP). If you select a general protocol such as `ip`, `tcp`, or `udp` the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as `http`, `https`, or `ssl` you can apply additional server load balancing features such as persistence and HTTP multiplexing.

- `http` load balance only HTTP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 80 for HTTP sessions). You can also configure `httpmultiplex`. You can also set persistence to `http-cookie` and configure `http-cookiedomain`, `http-cookie-path`, `http-cookiegeneration`, `http-cookie-age`, and `httpcookie-share` settings for cookie persistence.
- `https` load balance only HTTPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 443 for HTTPS sessions). You can also configure `httpmultiplex` and set persistence to `httpcookie` and configure the same `http-cookie` options as for `http` virtual servers plus the `httpscookie-secure` option. You can also set persistence to `ssl-`

`session-id`. You can also configure the SSL options such as `ssl-mode` and `ssl-certificate` and so on. `https` is available on FortiGate units that support SSL acceleration.

- `imaps` load balance only IMAPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 993 for IMAPS sessions).
- `ip` load balance all sessions accepted by the firewall policy that contains this server load balance virtual IP. Since all sessions are load balanced you don't have to set the `extport`.
- `pop3s` load balance only POP3S sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 995 for POP3S sessions).
- `smtps` load balance only SMTPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced (usually port 465 for SMTPS sessions).
- `ssl` load balance only SSL sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced. You can also configure the SSL options such as `ssl-mode` and `ssl-certificate` and so on.
- `tcp` load balance only TCP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced.
- `udp` load balance only UDP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced.

persistence {none | http-cookie | ssl-session-id}

If the `type` is `server-load-balance`, configure persistence for a virtual server to make sure that clients connect to the same server every time they make a request that is part of the same session. When you configure persistence, the FortiGate load balances a new session to a real server according to the `ldb-method`. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server. Persistence is disabled by default. You can configure persistence if `server-type` is set to `http`, `https`, or `ssl`. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server. Persistence is disabled by default. You can configure persistence if `server-type` is set to `http`, `https`, or `ssl`.

- `none` No persistence. Sessions are distributed solely according to the `ldb-method`. Setting `ldbmethod` to `static` (the default) results in behavior equivalent to persistence.
- `http-cookie` all HTTP or HTTPS sessions with the same HTTP session cookie are sent to the same real server. `http-cookie` is available if `server-type` is set to `https` or `ssl`. If you select this option you can also configure `httpcookie-domain`, `http-cookie-path`, `httpcookie-generation`, `http-cookie-age`, and `http-cookie-share` for HTTP and these settings plus `https-cookie-secure` for HTTPS.
- `ssl-session-id` all sessions with the same SSL session ID are sent to the same real server. `sslsession-id` is available if `server-type` is set to `https` or `ssl`.

nat-source-vip {disable | enable}

Enable (the default) to prevent unintended servers from using a virtual IP. The virtual IP will be used as the source IP address for connections from the server through the FortiGate.

Disable to use the actual IP address of the server (or the FortiGate destination interface if using NAT) as the source address of connections from the server that pass through the FortiGate unit.

portforward {disable | enable}

Select to enable port forwarding. You must also specify the port forwarding mappings by configuring `extport` and `mappedport`. Disabled by default.

protocol {sctp | tcp | udp | icmp}

Select the protocol to use when forwarding packets. The default is `tcp`.

extport <port-number>

External port number range that you want to map to a port number range on the destination network.

This option only appears if `portforward` is enabled. If `portforward` is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set `extport` to the port number range. Then set `mappedport` to the start and end of the destination port range.

When using port number ranges, the external port number range corresponds to a mapped port number range containing an equal number of port numbers, and each port number in the external range is always translated to the same port number in the mapped range.

If `type` is `server-load-balance`, `extport` is available unless `server-type` is `ip`. The value of `extport` changes to 80 if `server-type` is `http` and to 443 if `server-type` is `https`.

config realservers

The following are the options for `config realservers`, and are available only if `type` is `server-load-balance`.

ip <server-ip>

Enter the IP address of a server in this server load balancing cluster.

port

Enter the port used if port forwarding is enabled.

status {active | disable | standby}

Select whether the server is in the pool of servers currently being used for server load balanced traffic, the server is on standby, or is disabled. Default is `active`.

- `active` The FortiGate unit may forward traffic to the server unless its health check monitors determine that the server is unresponsive, at which time the FortiGate unit temporarily uses a server whose `status` is `standby`. The healthcheck monitor will continue to monitor the unresponsive server for the duration of `holddown-interval`. If this server becomes reliably responsive again, it will be restored to active use, and the standby server will revert to `standby`.
- `disable` The FortiGate unit does not forward traffic to this server, and does not perform health checks. You might use this option to conserve server load balancing resources when you know that a server will be unavailable for a long period, such as when the server is down for repair.
- `standby` If a server whose `status` is `active` becomes unresponsive, the FortiGate temporarily uses a responsive server whose `status` is `standby` until the server whose `status` is `active` again becomes reliably responsive. If multiple responsive `standby` servers are available, the FortiGate selects the standby server with the greatest weight. If a standby server becomes unresponsive, the FortiGate selects another responsive server whose `status` is `standby`.

holddown-interval <interval>

Enter the amount of time in seconds that the health check monitor continues to monitor the status of a server whose `status` is `active` after it has been detected to be unresponsive. Default is 300 seconds. If the server is detected to be continuously responsive during this interval, a server whose `status` is `standby` is removed from current use and replaced with this server, which is then used by server load balanced traffic. In this way, server load balancing prefers to use active servers, if they are responsive. If the server is detected to be unresponsive during the first holddown interval, the server remains out of use for server load balanced traffic, the health check monitor will double the holddown interval once, and continue to monitor the server for the duration of the doubled holddown interval. The health check monitor continues to monitor the server for additional iterations of the doubled holddown interval until connectivity to the server becomes reliable, at which time the holddown interval reverts to the configured interval, and the newly responsive active server replaces the standby server in the pool of servers currently in use. In effect, if the status of a server is `active` but the server is habitually unresponsive, the health check monitor is less likely to restore the server to use by server load balanced traffic until the server's connectivity becomes more reliable. This option applies only to real servers whose `status` is `active`, but have been detected to be unresponsive or down.

healthcheck {disable | enable}

Enable to check the responsiveness of the server before forwarding traffic. You must also configure `monitor`. Disabled by default.

max-connections <number>

Enter the limit on the number of active connections directed to a real server. If the maximum number of connections is reached for the real server, the FortiGate unit will automatically switch all further connection requests to another server until the connection number drops below the specified limit. The default of 0 means unlimited connections.

client-ip <ip_range_ipv4> [<ip_range_ipv4>] [<ip_range_ipv4>] [<ip_range_ipv4>]

Restrict the clients that can connect to a real server according to the client's source IP address. Use the `client-ip` option to enter up to four client source IP addresses or address ranges. Separate each IP address or range with a space. The following example shows how to add a single IP address and an IP address range:

```
set client-ip 192.168.1.90 192.168.1.100-192.168.1.120
```

Use the `client-ip` option if you have multiple real servers in a server load balance VIP and you want to control which clients use which real server according to the client's source IP address. Different real servers in the same virtual server can have the same or overlapping IP addresses and ranges. If an overlap occurs, sessions from the overlapping source addresses are load balanced among the real servers with the overlapping addresses. If you do not specify a `client-ip` all clients can use the real server.

weight <weight>

Enter the weight value of a specific server. Servers with a greater weight receive a greater proportion of forwarded connections, or, if their `status` is `standby`, are more likely to be selected to temporarily replace servers whose `status` is `active`, but that are unresponsive. Valid weight values are between 1 and 255. Default is 1. This option is available only if `ldb-method` is `weighted`.

mappedport <port>

Enter the port number range on the destination network to which the external port number range is mapped. You can also enter a port number range to forward packets to multiple ports on the destination network.

gratuitous-arp-interval <time>

Configure sending of gratuitous ARP packets by a virtual IP. You can set the time interval between sending the packets. The default is 0, which disables this feature.

srcintf-filter <interface> [<interface>...]

Enter names of the interfaces to which the VIP applies. Separate names with spaces.

http-cookie-domain-from-host {enable | disable}

If enabled, when the FortiGate unit adds a SetCookie to the HTTP(S) response, the Domain attribute in the SetCookie is set to the value of the Host: header, if there was one. If there was no Host: header, the Domain attribute is set to the value of `http-cookie-domain` if it is set and if it is not then the Domain attribute will not be included in the SetCookie. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http-cookie`. Enabled by default.

http-cookie-domain <domain>

Configure HTTP cookie persistence to restrict the domain that the cookie should apply to. Enter the domain name to restrict the cookie to. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

http-cookie-path <path>

Configure HTTP cookie persistence to limit the cookies to a particular path, for example `/new/path`. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

http-cookie-generation <generation>

Configure HTTP cookie persistence to invalidate all cookies that have already been generated. The exact value of the generation is not important, only that it is different from any generation that has already been used. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

http-cookie-age <age>

Configure HTTP cookie persistence to change how long the browser caches the cookie. Enter an age in minutes or set the age to 0 to make the browser keep the cookie indefinitely. The range is 0 to 525600 minutes. The default age is 60 seconds. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

http-cookie-share {disable | same-ip}

Configure HTTP cookie persistence to control the sharing of cookies across more than one virtual server. The default setting `same-ip` means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain. Disable to make sure that a cookie generated for a virtual server cannot be used by other virtual servers. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

https-cookie-secure {disable | enable}

Configure HTTP cookie persistence to enable or disable using secure cookies for HTTPS sessions. Secure cookies are disabled by default because they can interfere with cookie sharing across HTTP and HTTPS virtual servers. If enabled, then the Secure tag is added to the cookie inserted by the FortiGate unit. This option is available when `type` is `server-loadbalance`, `server-type` is `http` or `https` and `persistence` is `http` or `https`.

http-multiplex {disable | enable}

Enable to use the FortiGate to multiplex multiple client connections into a few connections between the FortiGate and the real server. This can improve performance by reducing server overhead associated with establishing multiple connections. The server must be HTTP/1.1 compliant. Disabled by default. This option is only available if `server-type` is `http` or `https`.

http-ip-header {disable | enable}

In HTTP multiplexing is enabled, set `http-ip-header` to `enable` to add the original client IP address in the `XForwarded-For` HTTP header. This can be useful in an HTTP multiplexing configuration if you want to be able to see the original client IP address in log messages on the destination web server. If this option is disabled, the HTTP header. This can be useful in an HTTP multiplexing configuration if you want to be able to see the original client IP address in log messages on the destination web server. If this option is disabled, the `XForwarded-For` header will contain the IP address of the FortiGate unit. Disabled by default. If enabled the `http-ip-header-name` option appears and you can specify a different header to add the client IP address to. This option appears only if `type` is `server-load-balance`, `server-type` is `http` or `https` and `http-multiplex` is enabled.

http-ip-header-name <name>

In an HTTP multiplex configuration, if you enable `http-ip-header` you can use the `http-ip-header-name` option to add the original client IP address to a custom http header. Use this option to specify the name of the header to add the IP address to. The destination server extracts the original client IP address from this header to record log messages that include client IP addresses. If you leave this option blank (the default) the original client IP address is added to the `XForwarded-For` header. This option appears only if `type` is `server-load-balance`, `server-type` is `http` or `https` and `http-multiplex` is enabled and `http-ip-header` is enabled.

outlook-web-access {disable | enable}

If the FortiGate unit provides SSL offloading for Microsoft Outlook Web Access then the Outlook server expects to see a `Front-End-Https: on` header inserted into the HTTP headers as described in this [Microsoft Technical Note](#). If `outlook-web-access` is enabled the FortiGate adds this header to all HTTP requests. Disabled by default. This options is available when `type` is `server-load-balance` is enabled and `server-type` is `http` or `https`.

weblogic-server {disable | enable}

Enable or disable adding an HTTP header to indicate SSL offloading for a WebLogic server. Disabled by default.

websphere-server {disable | enable}

Enable or disable adding an HTTP header to indicate SSL offloading for a WebSphere server. Disabled by default.

ssl-mode {full | half}

Select whether or not to accelerate SSL communications with the destination by using the FortiGate to perform SSL operations, and indicate which segments of the connection will receive SSL offloading. Accelerating SSL communications in this way is also called SSL offloading.

- `half` (the default) apply SSL acceleration only between the client and the FortiGate. The segment between the FortiGate and the server is clear text. This results in better performance, but cannot be used in failover configurations where the failover path does not have an SSL accelerator.
- `full` apply SSL acceleration to both parts of the connection: the segment between the client and the FortiGate, and the segment between the FortiGate and the server. The segment between the FortiGate and the server is encrypted, but the handshakes are accelerated. This results in performance which is less than if `ssl-mode` is set to `half`, but still improved over no SSL acceleration, and can be used in failover configurations where the failover path does not have an SSL accelerator. If the server is already configured to use SSL, this also enables SSL acceleration without requiring changes to the server's configuration. If this option is set to `full` then several `ssl-server` options appear and you can apply different SSL features (such as encryption levels) to the client connection and to the server connection.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

ssl-certificate <name>

The name of the SSL certificate to use for SSL acceleration. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full`, the same certificate is used for client and server communication.

ssl-dh-bits <bits>

Enter the number of bits used in the Diffie-Hellman exchange for RSA encryption of the SSL connection. Larger prime numbers are associated with greater cryptographic strength. Default is 2048. Values include 768, 1024, 1536, 2048, 3072, and 4096. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full`, the `ssl-dh-bits` setting is used for client and server communication.

ssl-algorithm {high | medium | low | custom}

Set the permitted encryption algorithms for SSL sessions according to encryption strength.

- `high` (the default) permit only high encryption algorithms: AES or 3DES.
- `medium` permit high (AES, 3DES) or medium (RC4) algorithms.

- `low` permit high (AES, 3DES), medium (RC4), or low (DES) algorithms.
- `custom` only allow some cipher suites to be used. Use `config ssl-cipher-suites` to select the cipher suites that are allowed.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full` and `ssl-server-algorithm` is set to `client`, the `ssl-algorithm` setting applies to both client and server communication. If `ssl-server-algorithm` is not set to `client`, the `ssl-algorithm` setting only applies to client communication. You can use the `ssl-server-algorithm` option to select different algorithms for server communication.

config ssl-cipher-suites

Choose one or more SSL cipher suites to use for SSL sessions. Only available if `ssl-algorithm` is set to `custom`. You can also use this command to list the supported SSL cipher suites available to all FortiOS SSL encryption/decryption applications.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full` and `ssl-server-algorithm` is set to `client`, the configured setting applies to both client and server communication.

If `ssl-server-algorithm` is not set to `client`, the `config ssl-cipher-suites` configuration only applies to client communication. You can use `config ssl-cipher-suites` to select different cipher suites for server communication.

cipher <cipher-suite-name>

Set the cipher suite name to use. Use `?` to list the available cipher suite names.

versions {ssl-3.0 | tls-1.0 | tls-1.1}

Select the SSL/TLS versions that are supported.

ssl-server-algorithm {high | medium | low | custom}

Set the permitted encryption algorithms for SSL server sessions according to encryption strength.

- `high` (the default) permit only high encryption algorithms: AES or 3DES.
- `medium` permit high (AES, 3DES) or medium (RC4) algorithms.
- `low` permit high (AES, 3DES), medium (RC4), or low (DES) algorithms.
- `custom` only allow some cipher suites to be used. Use `config ssl-server-cipher-suites` to select the cipher suites that are allowed.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-mode` is `full`.

config ssl-server-cipher-suites

Choose one or more SSL cipher suites to use for SSL server sessions. Only available if `ssl-server-algorithm` is set to `custom`. You can also use this command to list the supported SSL cipher suites available to all FortiOS SSL encryption/decryption applications.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, `ssl-mode` is `full`, and `ssl-server-algorithm` is `custom`.

cipher <cipher-suite-name>

Set the cipher suite name to use. Use `?` to list the available cipher suite names.

versions {ssl-3.0 | tls-1.0 | tls-1.1}

Select the SSL/TLS versions that are supported.

ssl-pfs {allow | deny | require}

Select handling of perfect forward secrecy (PFS) by controlling the cipher suites that can be selected. Applies to both client and server sessions.

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

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-algorithm` is not set to `custom`.

ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}

The lowest version of SSL/TLS to allow in SSL sessions. Default is `tls-1.0`. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full` and `ssl-server-min-version` is set to `client`, the configured setting applies to both client and server communication. If `ssl-server-min-version` is not set to `client`, this option only applies to client communication.

ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2}

The highest version of SSL/TLS to allow in SSL sessions. Default is `tls-1.2`. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`. If `ssl-mode` is set to `full` and `ssl-server-max-version` is set to `client`, the configured setting applies to both client and server communication. If `ssl-server-max-version` is not set to `client`, this option only applies to client communication.

ssl-server-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | client}

The lowest version of SSL/TLS to allow in SSL server sessions. Default is `client` which means the `ssl-min-version` applies to both client and server sessions. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-mode` is set to `full`.

ssl-server-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 | client}

The highest version of SSL/TLS to allow in SSL server sessions. Default is `client` which means the `ssl-max-version` applies to both client and server sessions. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and `ssl-mode` is set to `full`.

ssl-send-empty-frags {disable | enable}

Select to precede the record with empty fragments to thwart attacks on CBC IV. You might disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments. Enabled by default. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`, and applies only to SSL 3.0 and TLS 1.0.

ssl-client-fallback {disable | enable}

Enable (the default) to prevent Downgrade Attacks on client connections ([RFC 7507](#)). This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

ssl-client-renegotiation {allow | deny | secure}

Select the SSL secure renegotiation policy. Secure renegotiation complies with [RFC 5746](#) Secure Negotiation Indication. The vulnerability [CVE-2009-3555](#) affects all SSL/TLS servers that support re-negotiation. FortiOS when configured for SSL/TLS offloading is operating as a SSL/TLS server. The IETF is working on a TLS protocol change that will fix the problem identified by [CVE-2009-3555](#) while still supporting re-negotiation. Until that protocol change is available, you can use the `ssl-client-renegotiation` option to disable support for SSL/TLS re-negotiation.

- `allow` (the default) allow, but do not require secure renegotiation.
- `deny` do not allow renegotiation.
- `secure` require secure renegotiation.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

ssl-client-session-state-type {both | client | disable | time}

The method the FortiGate should use to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.

- **both** (the default) expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first.
- **count** expire SSL session states when `ssl-client-session-state-max` is exceeded.
- **disable** expire all SSL session states.
- **time** expire SSL session states when `ssl-client-session-state-timeout` is exceeded.

This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

ssl-client-session-state-timeout <timeout>

The number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the FortiGate unit. Default is 30 minutes. Range is 1 to 14400. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

ssl-client-session-state-max <states>

The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit. Default is 1000. Range is 0 to 100000. This option appears only if `type` is `server-loadbalance` and `server-type` is `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

ssl-server-session-state-type {both | count | disable | time}

The method the FortiGate should use to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.

- **both** (the default) expire SSL session states when either `ssl-server-session-state-max` or `ssl-server-session-state-timeout` is exceeded, regardless of which occurs first.
- **count** expire SSL session states when `ssl-server-session-state-max` is exceeded.
- **disable** expire all SSL session states.
- **time** expire SSL session states when `ssl-server-session-state-timeout` is exceeded.

This option appears only if `ssl-mode` is `full`.

ssl-server-session-state-timeout <time>

The number of minutes to keep the SSL session states for the segment of the SSL connection between the server and the FortiGate. Default is 30 minutes. Range is 1 to 14400. This option appears only if `ssl-mode` is `full`.

ssl-server-session-state-max

The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit. Default is 1000. Range is 0 to 100000. This option appears only if `ssl-mode` is `full`.

ssl-http-location-conversion {disable | enable}

Select to replace `http` with `https` in the reply's `Location` HTTP header field. For example, the reply, `Location: http://example.com/` would be converted to `Location: https://example.com/`. Disabled by default. This option appears only if `type` is `server-loadbalance` and `server-type` is `https`.

ssl-http-match-host {disable | enable}

Enable to apply `Location` conversion to the reply's HTTP header only if the host name portion of `Location` matches the request's `Host` field, or, if the `Host` field does not exist, the host name portion of the request's URI. If this option is disabled (the default), conversion occurs regardless of whether the host names in the request and the reply match. For example, if `ssl-http-match-host` is enabled, and a request contains `Host: example.com` and the reply contains `Location: http://example.cc/`, the `Location` field does not match the `Host` field of the original request and the reply's `Location` field remains unchanged. If the reply contains `Location: http://example.com/`, however, then the FortiGate detects the matching host name and converts the reply field to `Location: https://example.com/`. This option appears only if `type` is `server-loadbalance` and `server-type` is `https` and `ssl-http-location-conversion` is `enable`.

monitor <name>

The name of the health check monitor for use when polling to determine a virtual server's connectivity status.

max-embryonic-connections <number>

The maximum number of partially established SSL or HTTP connections. This should be greater than the maximum number of connections you want to establish per second. Default is 1000. Range is 0 to 100000. This option appears only if `type` is `server-loadbalance` and `server-type` is `http`, `ssl`, `https`, `imaps`, `pop3s`, or `smtps`.

portmapping-type {1-to-1 | m-to-n}

The type of port mapping.

- `1-to-1` one-to-one mapping (the default).
- `m-to-n` load balancing (many to many).

This option appears when `type` is not set to `server-load-balance`.

color <integer>

The color of the icon in the GUI. There are 32 defined colors numbered 1 to 32. To see the colors available, you can edit the VIP from the GUI. 1 is the default color which is black. 0 sets the color to the default color.

firewall {vip46 | vip64}

Introduction.

```
config firewall vip46
  edit { name }
  # Configure IPv4 to IPv6 virtual IPs.
  set name { string }   VIP46 name. size[63]
  set id { integer }    Custom defined id. range[0-65535]
  set uuid { uuid }     Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set comment { string } Comment. size[255]
  set type { static-nat | server-load-balance }  VIP type: static NAT or server load balance.
    static-nat          Static NAT.
    server-load-balance Server load balance.
  config src-filter
    edit { range }
    # Source IP filter (x.x.x.x/x).
    set range { string }  Src-filter range. size[79]
    next
  set extip { string }   Start-external-IP [-end-external-IP].
  set mappedip { string } Start-mapped-IP [-end mapped-IP].
  set arp-reply { disable | enable }  Enable ARP reply.
  set portforward { disable | enable } Enable port forwarding.
  set protocol { tcp | udp }  Mapped port protocol.
    tcp TCP.
    udp UDP.
  set extport { string } External service port.
  set mappedport { string } Mapped service port.
  set color { integer } Color of icon on the GUI. range[0-32]
  set ldb-method { option } Load balance method.
    static          Distribute sessions based on source IP.
    round-robin     Distribute sessions based round robin order.
    weighted        Distribute sessions based on weight.
    least-session   Distribute sessions to the server with the lowest session count.
    least-rtt       Distribute sessions to the server with the lowest Round-Trip-Time.
    first-alive     Distribute sessions to the first server that is alive.
  set server-type { http | tcp | udp | ip }  Server type.
    http HTTP
    tcp  TCP
```



```

        udp    UDP
        ip     IP
config realservers
  edit { id }
    # Real servers.
    set id { integer }   Real server ID. range[0-4294967295]
    set ip { ipv6 prefix } Mapped server IPv6.
    set port { integer }  Mapped server port. range[1-65535]
    set status { active | standby | disable }  Server administrative status.
        active  Server status active.
        standby Server status standby.
        disable Server status disable.
    set weight { integer }  weight range[1-255]
    set holddown-interval { integer }  Hold down interval. range[30-65535]
    set healthcheck { disable | enable | vip }  Per server health check.
    set max-connections { integer }  Maximum number of connections allowed to server. range[0-2147483647]
    set monitor { string }  Health monitors. size[64] - datasource(s): firewall.ldb-monitor.name
    set client-ip { string }  Restrict server to a client IP in this range.
  next
config monitor
  edit { name }
    # Health monitors.
    set name { string }  Health monitor name. size[64] - datasource(s): firewall.ldb-monitor.name
  next
next
end

config firewall vip64
  edit { name }
    # Configure IPv6 to IPv4 virtual IPs.
    set name { string }  VIP64 name. size[63]
    set id { integer }  Custom defined id. range[0-65535]
    set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
    set comment { string }  Comment. size[255]
    set type { static-nat | server-load-balance }  VIP type: static NAT or server load balance.
        static-nat      Static NAT.
        server-load-balance  Server load balance.
  config src-filter
    edit { range }
      # Source IP6 filter (x:x:x:x:x:x/x).
      set range { string }  Src-filter range. size[79]
    next

```

```
set extip { string } Start-external-IP [-end-external-IP].
set mappedip { string } Start-mapped-IP [-end-mapped-IP].
set arp-reply { disable | enable } Enable ARP reply.
set portforward { disable | enable } Enable port forwarding.
set protocol { tcp | udp } Mapped port protocol.
    tcp TCP.
    udp UDP.
set extport { string } External service port.
set mappedport { string } Mapped service port.
set color { integer } Color of icon on the GUI. range[0-32]
set ldb-method { option } Load balance method.
    static      Distribute sessions based on source IP.
    round-robin Distribute sessions based round robin order.
    weighted    Distribute sessions based on weight.
    least-session Distribute sessions to the server with the lowest session count.
    least-rtt   Distribute sessions to the server with the lowest Round-Trip-Time.
    first-alive Distribute sessions to the first server that is alive.
set server-type { http | tcp | udp | ip } Server type.
    http HTTP
    tcp  TCP
    udp  UDP
    ip   IP
config realservers
    edit { id }
        # Real servers.
        set id { integer } Real server ID. range[0-4294967295]
        set ip { ipv4 address any } Mapped server IP.
        set port { integer } Mapped server port. range[1-65535]
        set status { active | standby | disable } Server administrative status.
            active Server status active.
            standby Server status standby.
            disable Server status disable.
        set weight { integer } weight range[1-255]
        set holddown-interval { integer } Hold down interval. range[30-65535]
        set healthcheck { disable | enable | vip } Per server health check.
        set max-connections { integer } Maximum number of connections allowed to server. range[0-2147483647]
        set monitor { string } Health monitors. size[64] - datasource(s): firewall.ldb-monitor.name
        set client-ip { string } Restrict server to a client IP in this range.
    next
config monitor
    edit { name }
        # Health monitors.
        set name { string } Health monitor name. size[64] - datasource(s): firewall.ldb-monitor.name
```

```
    next
  next
end
```

firewall {vipgrp | vipgrp6}

Introduction.

```
config firewall vipgrp
  edit { name }
  # Configure IPv4 virtual IP groups.
  set name { string }  VIP group name. size[63]
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set interface { string }  interface size[35] - datasource(s): system.interface.name
  set color { integer }  Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).
range[0-32]
  set comments { string }  Comment. size[255]
  config member
  edit { name }
  # Member VIP objects of the group (Separate multiple objects with a space).
  set name { string }  VIP name. size[64] - datasource(s): firewall.vip.name
  next
next
end

config firewall vipgrp6
  edit { name }
  # Configure IPv6 virtual IP groups.
  set name { string }  IPv6 VIP group name. size[63]
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set color { integer }  Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).
range[0-32]
  set comments { string }  Comment. size[255]
  config member
  edit { name }
  # Member VIP objects of the group (Separate multiple objects with a space).
  set name { string }  IPv6 VIP name. size[64] - datasource(s): firewall.vip6.name
  next
next
end
```

firewall {vipgrp46 | vipgrp64}

Introduction.

```

config firewall vipgrp46
  edit { name }
  # Configure IPv4 to IPv6 virtual IP groups.
  set name { string }  VIP46 group name. size[63]
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set color { integer }  Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).
range[0-32]
  set comments { string }  Comment. size[255]
  config member
  edit { name }
  # Member VIP objects of the group (Separate multiple objects with a space).
  set name { string }  VIP46 name. size[64] - datasource(s): firewall.vip46.name
  next
next
end

config firewall vipgrp64
  edit { name }
  # Configure IPv6 to IPv4 virtual IP groups.
  set name { string }  VIP64 group name. size[63]
  set uuid { uuid }  Universally Unique Identifier (UUID; automatically assigned but can be manually reset).
  set color { integer }  Integer value to determine the color of the icon in the GUI (range 1 to 32, default = 0, which sets the value to 1).
range[0-32]
  set comments { string }  Comment. size[255]
  config member
  edit { name }
  # Member VIP objects of the group (Separate multiple objects with a space).
  set name { string }  VIP64 name. size[64] - datasource(s): firewall.vip64.name
  next
next
end

```

ftp-proxy

Use this command to

This section includes syntax for the following command:

- `ftp-proxy explicit`

ftp-proxy explicit

Introduction.

```
config ftp-proxy explicit
  set status { enable | disable }  Enable/disable the explicit FTP proxy.
  set incoming-port { string }  Accept incoming FTP requests on one or more ports.
  set incoming-ip { ipv4 address any }  Accept incoming FTP requests from this IP address. An interface must have this IP address.
  set outgoing-ip { ipv4 address any }  Outgoing FTP requests will leave from this IP address. An interface must have this IP address.
  set sec-default-action { accept | deny }  Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.
    accept  Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not
    deny    Deny requests unless there is a matching explicit FTP proxy policy.
end
```

icap

Use these commands to configure ICAP profiles and servers.

This section includes syntax for the following commands:

- [icap profile](#)
- [icap server](#)

icap profile

Introduction.

```
config icap profile
  edit { name }
  # Configure ICAP profiles.
  set replacemsg-group { string } Replacement message group. size[35] - datasource(s): system.replacemsg-group.name
  set name { string } ICAP profile name. size[35]
  set request { disable | enable } Enable/disable whether an HTTP request is passed to an ICAP server.
  set response { disable | enable } Enable/disable whether an HTTP response is passed to an ICAP server.
  set streaming-content-bypass { disable | enable } Enable/disable bypassing of ICAP server for streaming content.
  set request-server { string } ICAP server to use for an HTTP request. size[35] - datasource(s): icap.server.name
  set response-server { string } ICAP server to use for an HTTP response. size[35] - datasource(s): icap.server.name
  set request-failure { error | bypass } Action to take if the ICAP server cannot be contacted when processing an HTTP request.
    error Error.
    bypass Bypass.
  set response-failure { error | bypass } Action to take if the ICAP server cannot be contacted when processing an HTTP response.
    error Error.
    bypass Bypass.
  set request-path { string } Path component of the ICAP URI that identifies the HTTP request processing service. size[127]
  set response-path { string } Path component of the ICAP URI that identifies the HTTP response processing service. size[127]
  set methods { option } The allowed HTTP methods that will be sent to ICAP server for further processing.
    delete Forward HTTP request or response with DELETE method to ICAP server for further processing.
    get Forward HTTP request or response with GET method to ICAP server for further processing.
    head Forward HTTP request or response with HEAD method to ICAP server for further processing.
    options Forward HTTP request or response with OPTIONS method to ICAP server for further processing.
    post Forward HTTP request or response with POST method to ICAP server for further processing.
    put Forward HTTP request or response with PUT method to ICAP server for further processing.
    trace Forward HTTP request or response with TRACE method to ICAP server for further processing.
    other Forward HTTP request or response with All other methods to ICAP server for further processing.
  next
end
```

icap server

Introduction.

```
config icap server
  edit { name }
  # Configure ICAP servers.
  set name { string }  Server name. size[35]
  set ip-version { 4 | 6 }  IP version.
    4 IPv4 ICAP address.
    6 IPv6 ICAP address.
  set ip-address { ipv4 address any }  IPv4 address of the ICAP server.
  set ip6-address { ipv6 address }  IPv6 address of the ICAP server.
  set port { integer }  ICAP server port. range[1-65535]
  set max-connections { integer }  Maximum number of concurrent connections to ICAP server. range[1-65535]
next
end
```

ips

Use `ips` commands to configure IPS sensors to define which signatures are used to examine traffic and what actions are taken when matches are discovered. DoS sensors can also be defined to examine traffic for anomalies.

This section includes syntax for the following commands:

- `ips custom`
- `ips decoder`
- `ips global`
- `ips rule`
- `ips rule-settings`
- `ips sensor`
- `ips settings`

ips custom

The IPS sensors use signatures to detect attacks. The FortiGate's predefined signatures cover common attacks. These signatures can be listed with the `config ips rule ?` command. Details about the default settings of each signature can be displayed with the `get` command. If an unusual application or platform is being used, add custom signatures based on the security alerts released by the application and platform vendors. Custom signatures can be used to block or allow specific traffic and provide the power and flexibility to customize FortiGate Intrusion Protection for diverse network environments. You can only edit custom IPS signatures. A single custom signature can be used in multiple sensors with different settings in each.

```
config ips custom
  edit { tag }
  # Configure IPS custom signature.
  set tag { string }   Signature tag. size[63]
  set signature { string }   Custom signature enclosed in single quotes. size[1023]
  set sig-name { string }   Signature name. size[63]
  set rule-id { integer }   Signature ID. range[0-4294967295]
  set severity { string }   Relative severity of the signature, from info to critical. Log messages generated by the signature include the
severity.
  set location { string }   Protect client or server traffic.
  set os { string }   Operating system(s) that the signature protects. Blank for all operating systems.
  set application { string }   Applications to be protected. Blank for all applications.
  set protocol { string }   Protocol(s) that the signature scans. Blank for all protocols.
  set status { disable | enable }   Enable/disable this signature.
  set log { disable | enable }   Enable/disable logging.
  set log-packet { disable | enable }   Enable/disable packet logging.
  set action { pass | block }   Default action (pass or block) for this signature.
    pass   Pass or allow matching traffic.
    block  Block or drop matching traffic.
  set comment { string }   Comment. size[63]
next
end
```

Example config ips rule

This example shows how to display the current configuration of the MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures signature.

```
config ips rule MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
(MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures) # get
name                : MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
status              : enable
log                 : enable
log-packet          : disable
action              : block
group               : web_client
severity            : high
location            : server, client
os                  : Windows
application         : Other
service             : TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP
rule-id             : 42597
rev                 : 8.928
date                : 1472457600
```

signature <signature_str>

The custom signature enclosed in single quotes. For more information, see [Custom IPS Signature Syntax Guide](#).

severity {all | info | low | medium | high | critical}

Relative importance of signature, from info to critical. Log messages generated by the signature include the severity.

location {client | server}

Specify the type of system to be protected.

os {all | other | windows | linux | bsd | solaris | macos}

Operating system(s) that the signature protects. Blank (the default) for all operating systems.

- `all`: all operating systems included.
- `other`: all unlisted operating systems included.

application [<app1> <app2> ...]

Application(s) that the signature scans. `set application ?`: lists all applications in the current configuration. Blank (the default) for all applications.

protocol [<pro1> <pro2> ...]

Protocol(s) that the signature scans. `set protocol ?`: lists protocols and CLI syntax. Blank (the default) for all protocols

status {enable | disable}

Default status of the signature when it is included in an IPS Sensor. Default is `enable`.

log {enable | disable}

Enable/disable logging. Default is `enable`.

log-packet {enable | disable}

Enable/disable packet logging for this signature. Default is `disable`.

action {block | pass}

Default action for this signature. Default is `pass`.

comment <comment_str>

Description of the custom IPS signature. Appears in the profile list. Descriptions with spaces must be enclosed in quotes.

ips decoder

Introduction.

```
config ips decoder
  edit { name }
  # Configure IPS decoder.
  set name { string }  Decoder name. size[63]
  config parameter
    edit { name }
    # IPS group parameters.
    set name { string }  Parameter name. size[31]
    set value { string }  Parameter value. size[199]
  next
next
end
```

ips global

This command sets IPS global operating parameters.

```

config ips global
  set fail-open { enable | disable }  Enable to allow traffic if the IPS process crashes. Default is disable and IPS traffic is blocked when the
  IPS process crashes.
  set database { regular | extended }  Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Exten-
  ded includes protection from legacy attacks.
    regular  IPS regular database package.
    extended IPS extended database package.
  set traffic-submit { enable | disable }  Enable/disable submitting attack data found by this FortiGate to FortiGuard.
  set anomaly-mode { periodical | continuous }  Global blocking mode for rate-based anomalies.
    periodical  After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.
    continuous  Block packets once an anomaly is detected. Overrides individual anomaly settings.
  set session-limit-mode { accurate | heuristic }  Method of counting concurrent sessions used by session limit anomalies. Choose between greater
  accuracy (accurate) or improved performance (heuristics).
    accurate  Accurately count concurrent sessions, demands more resources.
    heuristic  Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.
  set intelligent-mode { enable | disable }  Enable/disable IPS adaptive scanning (intelligent mode). Intelligent mode optimizes the scanning
  method for the type of traffic.
  set socket-size { integer }  IPS socket buffer size (1 - 256 MB). Default depends on available memory. Can be changed to tune performance. range
  [1-256]
  set engine-count { integer }  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. range[0-255]
  set sync-session-ttl { enable | disable }  Enable/disable use of kernel session TTL for IPS sessions.
  set np-accel-mode { none | basic }  Acceleration mode for IPS processing by NPx processors.
    none  NPx acceleration disabled.
    basic NPx acceleration enabled.
  set ips-reserve-cpu { disable | enable }  Enable/disable IPS daemon's use of CPUs other than CPU 0
  set cp-accel-mode { none | basic | advanced }  IPS Pattern matching acceleration/offloading to CPx processors.
    none  CPx acceleration/offloading disabled.
    basic  Offload basic pattern matching to CPx processors.
    advanced  Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.
  set skype-client-public-ipaddr { string }  Public IP addresses of your network that receive Skype sessions. Helps identify Skype sessions. Separ-
  ate IP addresses with commas. size[255]
  set deep-app-insp-timeout { integer }  Timeout for Deep application inspection (1 - 2147483647 sec., 0 = use recommended setting). range[0-
  2147483647]
  set deep-app-insp-db-limit { integer }  Limit on number of entries in deep application inspection database (1 - 2147483647, 0 = use recommended

```



```
setting) range[0-2147483647]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

fail-open {enable | disable}

`enable fail-open` ensures that, if IPS should cease to function, crucial network traffic will not be blocked and firewall will continue to operate while the problem is resolved. Default is `disable` which means that if the IPS process fails, IPS traffic is blocked.

database {regular | extended}

Identify which IPS database to use. Default is `regular`. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.

traffic-submit {enable | disable}

Enable/disable submission of attack characteristics to FortiGuard Service. Default is `disable`.

anomaly-mode {continuous | periodical}

Specify blocking mode for rate-based anomaly. Default is `continuous`.

- `continuous` after an anomaly is detected, allow the configured number of packets per second.
- `periodical` block all packets once an anomaly is detected. Overrides individual anomaly settings.

session-limit-mode {accurate | heuristic}

Select the method that session limit anomalies use to estimate concurrent sessions. Use these options to choose between optimal performance and more accurate information. Default is `heuristic`.

- `accurate` accurately count the concurrent sessions. This option requires more resources than the default heuristics method
- `heuristic` uses heuristics to estimate concurrent sessions. Results may be less accurate but acceptable in most cases.

intelligent-mode {enable | disable}

Enable/disable IPS adaptive scanning (intelligent mode). Intelligent mode optimizes the scanning method for the type of traffic. Default is `enable`.

socket-size <ips_buffer_size>

Intrusion protection buffer size in MB. Default varies by model depending on available physical memory. Can be changed to tune performance.

engine-count {integer}

Number of intrusion protection engines to run. Default is 0. Multi-processor FortiGate units can more efficiently process traffic with multiple engines running. When set to the default value of 0, the FortiGate unit determines the optimal number of intrusion protection engines.

algorithm {engine-pick | low | high | super}

Specify the method used by the IPS engine for determining whether traffic matches signatures. Default is `engine-pick`.

- `engine-pick` allows the IPS engine to choose the best method
- `low` is a slower method that uses less memory
- `high` is a faster method that uses more memory
- `super` is a method that works well on models with more than 4GB memory

sync-session-ttl {enable | disable}

Enable/disable use of kernel session TTL for IPS sessions. Default is `disable`.

np-accel-mode {none | basic}

Acceleration mode for IPS processing by NPx processors.

- `none`: NP acceleration disabled.
- `basic`: NP acceleration enabled.

cp-accel-mode {none | basic | advanced}

CP8 or CP9 acceleration/offloading of pattern matching. For more information see [Hardware Acceleration Overview](#).

- `none` CP8 or CP9 acceleration disabled.
- `basic` offload basic pattern matching to CP8 or CP9 processors.
- `advanced` (the default) offloads more types of pattern matching resulting in higher throughput than basic mode. `advanced` is only available on FortiGate models with two or more CP8s or one or more CP9s.

skype-client-public-ipaddr <IP_addr_list>

Specify the public IP addresses of your network that receive Skype sessions. This will help the FortiGate unit identify Skype sessions properly in the Sessions dashboard widget and when attempting to detect/block them. Separate IP addresses with commas, not spaces.

deep-app-insp-timeout <seconds>

Sets number of seconds after which inactive application database entries are deleted. Range 1 - 2147483647. Default is 0, and sets recommended value.

deep-app-insp-db-limit <entries_int>

Set the maximum number of application database entries. Range: 1 - 2147483647. Default is 0, and sets recommended value.

exclude-signatures {none | industrial}

Excluded signatures don't appear on the GUI. Used for hiding industrial signatures, which are used by a specialized customer base. Default is `industrial`.

- `none`: no signatures excluded
- `industrial`: exclude industrial signatures

ips rule

The IPS sensors use signatures to detect attacks. The FortiGate's predefined signatures cover common attacks. These signatures can be listed with the `config ips rule ?` command. Details about the default settings of each signature can be displayed with the `get` command. If an unusual application or platform is being used, add custom signatures based on the security alerts released by the application and platform vendors. Custom signatures can be used to block or allow specific traffic and provide the power and flexibility to customize FortiGate Intrusion Protection for diverse network environments. You can only edit custom IPS signatures. A single custom signature can be used in multiple sensors with different settings in each.

```
config ips rule
  edit { name }
  # Configure IPS rules.
  set name { string } Rule name. size[63]
  set status { disable | enable } Enable/disable status.
  set log { disable | enable } Enable/disable logging.
  set log-packet { disable | enable } Enable/disable packet logging.
  set action { pass | block } Action.
    pass Pass or allow matching traffic.
    block Block or drop matching traffic.
  set group { string } Group. size[63]
  set os { string } Vulnerable operation systems.
  set application { string } Vulnerable applications.
  set service { string } Vulnerable service.
  set rule-id { integer } Rule ID. range[0-4294967295]
  set rev { integer } Revision. range[0-4294967295]
  set date { integer } Date. range[0-4294967295]
  config metadata
    edit { id }
    # Meta data.
    set id { integer } ID. range[0-4294967295]
    set metaid { integer } Meta ID. range[0-4294967295]
    set valueid { integer } Value ID. range[0-4294967295]
  next
end
```

Example config ips rule

This example shows how to display the current configuration of the MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures signature.

```
config ips rule MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
(MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures) # get
name                : MS.Edge.Windows.Data.Pdf.dll.Information.Disclosures
status              : enable
log                 : enable
log-packet          : disable
action              : block
group               : web_client
severity            : high
location            : server, client
os                  : Windows
application         : Other
service             : TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP
rule-id             : 42597
rev                 : 8.928
date                : 1472457600
```

signature <signature_str>

The custom signature enclosed in single quotes. For more information, see [Custom IPS Signature Syntax Guide](#).

severity {all | info | low | medium | high | critical}

Relative importance of signature, from info to critical. Log messages generated by the signature include the severity.

location {client | server}

Specify the type of system to be protected.

os {all | other | windows | linux | bsd | solaris | macos}

Operating system(s) that the signature protects. Blank (the default) for all operating systems.

- `all`: all operating systems included.
- `other`: all unlisted operating systems included.

application [<app1> <app2> ...]

Application(s) that the signature scans. `set application ?`: lists all applications in the current configuration. Blank (the default) for all applications.

protocol [<pro1> <pro2> ...]

Protocol(s) that the signature scans. `set protocol ?`: lists protocols and CLI syntax. Blank (the default) for all protocols.

status {enable | disable}

Default status of the signature when it is included in an IPS Sensor. Default is `enable`.

log {enable | disable}

Enable/disable logging. Default is `enable`.

log-packet {enable | disable}

Enable/disable packet logging for this signature. Default is `disable`.

action {block | pass}

Default action for this signature. Default is `pass`.

comment <comment_str>

Description of the custom IPS signature. Appears in the profile list. Descriptions with spaces must be enclosed in quotes.

ips rule-settings

Introduction.

```
config ips rule-settings
  edit { id }
  # Configure IPS rule setting.
  set id { integer } Rule ID. range[0-4294967295]
  config tags
    edit { name }
    # Applied object tags.
    set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
next
end
```

ips sensor

The IPS sensors use signatures to detect attacks. IPS sensors are made up of filters and override rules. Each filter specifies a number of signature attributes and all signatures matching all the specified attributes are included in the filter.

```

config ips sensor
  edit { name }
  # Configure IPS sensor.
  set name { string }  Sensor name. size[35]
  set comment { string }  Comment. size[255]
  set replacemsg-group { string }  Replacement message group. size[35] - datasource(s): system.replacemsg-group.name
  set block-malicious-url { disable | enable }  Enable/disable malicious URL blocking.
config entries
  edit { id }
  # IPS sensor filter.
  set id { integer }  Rule ID in IPS database (0 - 4294967295). range[0-4294967295]
  config rule
    edit { id }
    # Identifies the predefined or custom IPS signatures to add to the sensor.
    set id { integer }  Rule IPS. range[0-4294967295]
    next
  set location { string }  Protect client or server traffic.
  set severity { string }  Relative severity of the signature, from info to critical. Log messages generated by the signature include
the severity.
  set protocol { string }  Protocols to be examined. set protocol ? lists available protocols. all includes all protocols. other
includes all unlisted protocols.
  set os { string }  Operating systems to be protected. all includes all operating systems. other includes all unlisted operating sys-
tems.
  set application { string }  Applications to be protected. set application ? lists available applications. all includes all
applications. other includes all unlisted applications.
  config tags
    edit { name }
    # Assign a custom tag filter to the IPS sensor.
    set name { string }  Tag name. size[64] - datasource(s): system.object-tag.name
    next
  set status { disable | enable | default }  Status of the signatures included in filter. default enables the filter and only use fil-
ters with default status of enable. Filters with default status of disable will not be used.
  set log { disable | enable }  Enable/disable logging of signatures included in filter.
  set log-packet { disable | enable }  Enable/disable packet logging. Enable to save the packet that triggers the filter. You can

```


download the packets in pcap format for diagnostic use.

```

set log-attack-context { disable | enable }  Enable/disable logging of attack context: URL buffer, header buffer, body buffer,
packet buffer.
set action { pass | block | reset | default }  Action taken with traffic in which signatures are detected.
    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.
set rate-count { integer }  Count of the rate. range[0-65535]
set rate-duration { integer }  Duration (sec) of the rate. range[1-65535]
set rate-mode { periodical | continuous }  Rate limit mode.
    periodical  Allow configured number of packets every rate-duration.
    continuous  Block packets once the rate is reached.
set rate-track { option }  Track the packet protocol field.
    none        none
    src-ip      Source IP.
    dest-ip     Destination IP.
    dhcp-client-mac  DHCP client.
    dns-domain  DNS domain.
config exempt-ip
edit { id }
    # Traffic from selected source or destination IP addresses is exempt from this signature.
    set id { integer }  Exempt IP ID. range[0-4294967295]
    set src-ip { ipv4 classnet }  Source IP address and netmask.
    set dst-ip { ipv4 classnet }  Destination IP address and netmask.
next
set quarantine { none | attacker }  Quarantine method.
    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.
    set quarantine-expiry { string }  Duration of quarantine, from 1 minute to 364 days, 23 hours, and 59 minutes from now. (format:
###d##h##m, default = 5m). Requires quarantine set to attacker.
    set quarantine-log { disable | enable }  Enable/disable quarantine logging.
next
config filter
edit { name }
    # IPS sensor filter.
    set name { string }  Filter name. size[31]
    set location { string }  Vulnerability location filter.
    set severity { string }  Vulnerability severity filter.
    set protocol { string }  Vulnerable protocol filter.
    set os { string }  Vulnerable OS filter.
    set application { string }  Vulnerable application filter.

```

```

set status { disable | enable | default } Selected rules status.
set log { disable | enable } Enable/disable logging of selected rules.
set log-packet { disable | enable } Enable/disable packet logging of selected rules.
set action { pass | block | reset | default } Action of selected rules.
    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.
set quarantine { none | attacker } Quarantine IP or interface.
    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.

```

set quarantine-expiry { integer } Duration of quarantine in minute. range[1-2147483647]
set quarantine-log { disable | enable } Enable/disable logging of selected quarantine.

```

next

config override

```
edit { rule-id }
```

```
# IPS override rule.
```

```

set rule-id { integer } Override rule ID. range[0-4294967295]
set status { disable | enable } Enable/disable status of override rule.
set log { disable | enable } Enable/disable logging.
set log-packet { disable | enable } Enable/disable packet logging.
set action { pass | block | reset } Action of override rule.
    pass Pass or allow matching traffic.
    block Block or drop matching traffic.
    reset Reset sessions for matching traffic.

```

```

set quarantine { none | attacker } Quarantine IP or interface.
    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.

```

set quarantine-expiry { integer } Duration of quarantine in minute. range[1-2147483647]
set quarantine-log { disable | enable } Enable/disable logging of selected quarantine.

```

config exempt-ip

```
edit { id }
```

```
# Exempted IP.
```

```

set id { integer } Exempt IP ID. range[0-4294967295]
set src-ip { ipv4 classnet } Source IP address and netmask.
set dst-ip { ipv4 classnet } Destination IP address and netmask.

```

next

next

next

end

comment <comment_str>

Enter an optional comment to describe the sensor. This description will appear in the ISP sensor list. Descriptions with spaces must be enclosed in quotes.

replacemsg-group <replacemsg_str>

Specify the replacement message group.

block-malicious-url {enable | disable}

Enable/disable blocking of malicious URLs. Default is `disable`.

config entries**rule <rule1_int> [<rule2_int> <rule3_int> ...]**

Use rule ID to identify the predefined or custom IPS signatures to add to sensor.

location {all | client | server}

Specify the type of system to be protected. Default is `all`.

severity {all | info | low | medium | high | critical}

Relative importance of signature, from info to critical. Default is `all`.

protocol <prot1_str> [<prot2_str> <prot3_str> . . .]

Specify protocols to be examined.

- `?` lists available protocols.
- `all` includes all protocols.
- `other` includes all unlisted protocols

os {all | other | windows | linux | bsd | solaris | macos}

Specify operating systems to be protected. Default is `all`.

- `all` includes all operating systems.
- `other` includes all unlisted operating systems

application <app1_str> [<app2_str> <app3_str> . . .]

Specify applications to be protected.

- `?` lists available applications.
- `all` includes all applications.
- `other` includes all unlisted applications.

tags <tag_str>

Assign a custom tag filter to the IPS sensor. Tag must first be configured by using `config system object-tag`. To see what tags are available for use, use the command `set tags ?`. Separate multiple values with a space.

status {default | enable | disable}

Specify status of the signatures included in filter. Default is `default`.

- `default` enables the filter and only use filters with default status of `enable`. Filters with default status of `disable` will not be used.

log {default | enable | disable}

Specify the logging status of the signatures included in the filter. Default is `default`.

- `default` enable logging for only the filters with a default logging status of `enable`. Filters with a default logging status of `disable` will not be logged.

log-packet {enable | disable}

Enable/disable packet logging. `enable` saves the packet that triggers the filter. Default is `disable`.

You can download the packets in `pcap` format for diagnostic use. This feature is only available in FortiGate units with internal hard drives.

log-attack-context {default | enable | disable}

Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer. Default is `disable`.

action {block | default | pass | reject}

Specify what action is taken with traffic in which signatures are detected. Default is `default`.

- `block` will drop the session with offending traffic.
- `pass` allow the traffic.
- `reject` reset the session.
- `default` either pass or drop matching traffic, depending on the default action of each signature.

quarantine {attacker | none}

Specify how the FortiGate will quarantine attackers. Default is `none`.

- `attacker` blocks 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.
- `none` disables the adding of addresses to the quarantine.

config exempt-ip

This subcommand is available after rule has been set.

edit <exempt-ip_id>

Enter the ID number of an `exempt-ip` entry. For a list of the `exempt-ip` entries in the IPS sensor, enter `?` instead of an ID. Enter a new ID to create a new `exempt-ip`.

dst-ip <ip4mask>

Enter destination IP address and netmask to exempt.

src-ip <ip4mask>

Enter source IP address and netmask to exempt.

ips settings

This command configures settings for IPS packet logging.

```
config ips settings
    set packet-log-history { integer }    Number of packets to capture before and including the one in which the IPS signature is detected (1 - 255).
    range[1-255]
    set packet-log-post-attack { integer }    Number of packets to log after the IPS signature is detected (0 - 255). range[0-255]
    set packet-log-memory { integer }    Maximum memory can be used by packet log (64 - 8192 kB). range[64-8192]
    set ips-packet-quota { integer }    Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size. range
    [0-4294967295]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

packet-log-history <packets_int>

Specify number of packets to capture before and including the one in which the IPS signature is detected. Range: 0 - 255. Default is 1. If the value is more than 1, the packet containing the signature is saved in the packet log, as well as those preceding it. For example, if `packet-log-history` is set to 7, the FortiGate unit will save the packet containing the IPS signature match and the six before it.

Setting `packet-log-history` to a value larger than 1 can affect the performance of the FortiGate unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.

packet-log-post-attack <packets_int>

Specify how many packets to log after the IPS signature is detected. Range: 0 - 255. Default is 0. If `packet-log-post-attack` is set to 10, the FortiGate unit will save the ten packets following the one containing the IPS signature match.

packet-log-memory <KB_int>

Specify the maximum amount of memory to use for logging packets to memory. Acceptable range: 64 - 8192 KB. Default is 256.

ips-packet-quota <MB_int>

Specify maximum amount of disk space to use for logged packets when logging to disk. Range: 0 - 4294967295 MB. Default is 0. This command affects only logging to disk.

log

Use the config log commands to set the logging type, the logging severity level, and the logging location for the FortiGate unit.

This section includes syntax for the following commands:

- log custom-field
- log disk filter
- log disk setting
- log eventfilter
- log fortianalyzer override-filter
- log fortianalyzer override-setting
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log fortiguard filter
- log fortiguard override-filter
- log fortiguard override-setting
- log fortiguard setting
- log gui-display
- log memory filter
- log memory global-setting
- log memory setting
- log null-device filter
- log null-device setting
- log setting
- log syslogd override-filter
- log syslogd override-setting
- log {syslogd | syslogd2 | syslogd3 | syslogd4} filter
- log {syslogd | syslogd2 | syslogd3 | syslogd4} setting
- log threat-weight

-
- [log webtrends filter](#)
 - [log webtrends setting](#)

log custom-field

Use `log custom-field` to create custom fields that will be included with log messages. **Note:** 'id' will not appear in log messages, it is only used for database purposes.

```
config log custom-field
  edit { id }
  # Configure custom log fields.
  set id { string } field id { string }. size[35]
  set name { string } Field name (max: 15 characters). size[15]
  set value { string } Field value (max: 15 characters). size[15]
  next
end
```

edit <id>

A table value for custom fields in log messages. Edit to create new and configure the custom fields using the following entries:

name <name>

The name of the field, which will appear in log messages.

value <value>

The content of the field, which will appear in log messages.

log disk filter

Introduction.

```
config log disk filter
  set severity { option }  Log to disk every message above and including this severity level.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.

  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dlp-archive { enable | disable }  Enable/disable DLP archive logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set event { enable | disable }  Enable/disable event logging.
  set system { enable | disable }  Enable/disable system activity logging.
  set radius { enable | disable }  Enable/disable RADIUS messages logging.
  set ipsec { enable | disable }  Enable/disable IPsec negotiation messages logging.
  set dhcp { enable | disable }  Enable/disable DHCP service messages logging.
  set ppp { enable | disable }  Enable/disable L2TP/PPTP/PPPoE logging.
  set admin { enable | disable }  Enable/disable admin login/logout logging.
  set ha { enable | disable }  Enable/disable HA logging.
  set auth { enable | disable }  Enable/disable firewall authentication logging.
  set pattern { enable | disable }  Enable/disable pattern update logging.
  set sslvpn-log-auth { enable | disable }  Enable/disable SSL user authentication logging.
  set sslvpn-log-adm { enable | disable }  Enable/disable SSL administrator login logging.
  set sslvpn-log-session { enable | disable }  Enable/disable SSL session logging.
  set vip-ssl { enable | disable }  Enable/disable VIP SSL logging.
  set ldb-monitor { enable | disable }  Enable/disable VIP real server health monitoring logging.
  set wan-opt { enable | disable }  Enable/disable WAN optimization event logging.
  set wireless-activity { enable | disable }  Enable/disable wireless activity event logging.
```

```
set cpu-memory-usage { enable | disable } Enable/disable CPU & memory usage logging every 5 minutes.
set filter { string } Disk log filter. size[511]
set filter-type { include | exclude } Include/exclude logs that match the filter.
    include Include logs that match the filter.
    exclude Exclude logs that match the filter.
end
```

log disk setting

Introduction.

```
config log disk setting
  set status { enable | disable }  Enable/disable local disk logging.
  set ips-archive { enable | disable }  Enable/disable IPS packet archiving to the local disk.
  set max-log-file-size { integer }  Maximum log file size before rolling (1 - 100 Mbytes). range[1-100]
  set max-policy-packet-capture-size { integer }  Maximum size of policy sniffer in MB (0 means unlimited). range[0-4294967295]
  set roll-schedule { daily | weekly }  Frequency to check log file for rolling.
    daily  Check the log file once a day.
    weekly Check the log file once a week.
  set roll-day { option }  Day of week on which to roll log file.
    sunday  Sunday
    monday  Monday
    tuesday Tuesday
    wednesday Wednesday
    thursday Thursday
    friday  Friday
    saturday Saturday
  set roll-time { string }  Time of day to roll the log file (hh:mm).
  set diskfull { overwrite | nolog }  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).
    overwrite Overwrite the oldest logs when the log disk is full.
    nolog      Stop logging when the log disk is full.
  set log-quota { integer }  Disk log quota (MB). range[0-4294967295]
  set dlp-archive-quota { integer }  DLP archive quota (MB). range[0-4294967295]
  set report-quota { integer }  Report quota (MB). range[0-4294967295]
  set maximum-log-age { integer }  Delete log files older than (days). range[0-3650]
  set upload { enable | disable }  Enable/disable uploading log files when they are rolled.
  set upload-destination { ftp-server }  The type of server to upload log files too. Only FTP is currently supported.
    ftp-server Upload rolled log files to an FTP server.
  set uploadip { ipv4 address }  IP address of the FTP server to upload log files to.
  set uploadport { integer }  TCP port to use for communicating with the FTP server (default = 21). range[0-65535]
  set source-ip { ipv4 address }  Source IP address to use for uploading disk log files.
  set uploaduser { string }  Username required to log into the FTP server to upload disk log files. size[35]
  set uploadpass { password_string }  Password required to log into the FTP server to upload disk log files. size[128]
  set uploaddir { string }  The remote directory on the FTP server to upload log files to. size[63]
  set uploadtype { option }  Types of log files to upload. Separate multiple entries with a space.
```

```
traffic      Upload traffic log.
event        Upload event log.
virus        Upload anti-virus log.
webfilter    Upload web filter log.
IPS          Upload IPS log.
spamfilter   Upload spam filter log.
dlp-archive  Upload DLP archive.
anomaly      Upload anomaly log.
voip         Upload VoIP log.
dlp          Upload DLP log.
app-ctrl     Upload application control log.
waf          Upload web application firewall log.
netscan     Upload network vulnerability scanning log.
dns          Upload DNS log.
set uploadsched { disable | enable } Set the schedule for uploading log files to the FTP server (default = disable = upload when rolling).
set uploadtime { integer } Hour of the day on which log files are uploaded if uploadsched is enabled (0 - 23, default = 0). range[0-23]
set upload-delete-files { enable | disable } Delete log files after uploading (default = enable).
set upload-ssl-conn { default | high | low | disable } Enable/disable encrypted FTPS communication to upload log files.
    default  FTPS with high and medium encryption algorithms.
    high     FTPS with high encryption algorithms.
    low      FTPS with low encryption algorithms.
    disable  Disable FTPS communication.
set full-first-warning-threshold { integer } Log full first warning threshold as a percent (1 - 98, default = 75). range[1-98]
set full-second-warning-threshold { integer } Log full second warning threshold as a percent (2 - 99, default = 90). range[2-99]
set full-final-warning-threshold { integer } Log full final warning threshold as a percent (3 - 100, default = 95). range[3-100]
end
```

log eventfilter

Use `log eventfilter` to select which Event log messages will be recorded.

Note: `event` must be enabled for any of the other options to appear. Disabling it overrides all other enabled log types in this category.

```
config log eventfilter
  set event { enable | disable }  Enable/disable event logging.
  set system { enable | disable }  Enable/disable system event logging.
  set vpn { enable | disable }  Enable/disable VPN event logging.
  set user { enable | disable }  Enable/disable user authentication event logging.
  set router { enable | disable }  Enable/disable router event logging.
  set wireless-activity { enable | disable }  Enable/disable wireless event logging.
  set wan-opt { enable | disable }  Enable/disable WAN optimization event logging.
  set endpoint { enable | disable }  Enable/disable endpoint event logging.
  set ha { enable | disable }  Enable/disable ha event logging.
  set compliance-check { enable | disable }  Enable/disable PCI DSS compliance check logging.
  set security-audit { enable | disable }  Enable/disable Security Fabric audit result logging.
end
```

event {enable | disable}

Enable or disable logging of all Event logs, which track various FortiGate system and function events.

system {enable | disable}

Enable or disable logging of system activity messages, HA activity messages, CPU & memory usage, VIP realserver health monitoring, and AMC interface bypass mode messages.

vpn {enable | disable}

Enable or disable logging of VPN messages, IPSec negotiation messages, SSL user authentication, administration and session messages.

user {enable | disable}

Enable or disable logging of user authentication events.

router {enable | disable}

Enable or disable logging of router activity and state change events.

wireless-activity {enable | disable}

Enable or disable logging of wireless activity and state change events.

wan-opt {enable | disable}

Enable or disable logging of WAN Optimization activity and state change events.

endpoint {enable | disable}

Enable or disable logging of Endpoint Control activity and state change events.

ha {enable | disable}

Enable or disable logging of all HA activity and state change events.

compliance-check {enable | disable}

Enable or disable logging of all Compliance-related system events.

log fortianalyzer override-filter

Introduction.

```
config log fortianalyzer override-filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dlp-archive { enable | disable }  Enable/disable DLP archive logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  FortiAnalyzer log filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```

log fortianalyzer override-setting

Introduction.

```
config log fortianalyzer override-setting
  set override { enable | disable }  Enable/disable overriding FortiAnalyzer settings or use global settings.
  set use-management-vdom { enable | disable }  Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.
  set status { enable | disable }  Enable/disable logging to FortiAnalyzer.
  set ips-archive { enable | disable }  Enable/disable IPS packet archive logging.
  set server { string }  IPv4 or IPv6 address of the remote FortiAnalyzer. size[63]
  set hmac-algorithm { sha256 | sha1 }  FortiAnalyzer IPsec tunnel HMAC algorithm.
    sha256  Use SHA256 as HMAC algorithm.
    sha1    Step down to SHA1 as the HMAC algorithm.
  set enc-algorithm { high-medium | high | low | disable }  Enable/disable sending FortiAnalyzer log data with SSL encryption.
    high-medium  Encrypt logs using high and medium encryption algorithm.
    high         Encrypt logs using high encryption algorithm.
    low         Encrypt logs using low encryption algorithm.
    disable     Disable SSL encryption.
  set conn-timeout { integer }  FortiAnalyzer connection time-out in seconds (for status and log buffer). range[1-3600]
  set monitor-keepalive-period { integer }  Time between OFTP keepalives in seconds (for status and log buffer). range[1-120]
  set monitor-failure-retry-period { integer }  Time between FortiAnalyzer connection retries in seconds (for status and log buffer). range[1-86400]
  set mgmt-name { string }  Hidden management name of FortiAnalyzer. size[35]
  set faz-type { integer }  Hidden setting index of FortiAnalyzer. range[0-4294967295]
  set certificate { string }  Certificate used to communicate with FortiAnalyzer. size[35] - datasource(s): certificate.local.name
  set source-ip { string }  Source IPv4 or IPv6 address used to communicate with FortiAnalyzer. size[63]
  set __change_ip { integer }  Hidden attribute. range[0-255]
  set upload-option { store-and-upload | realtime | 1-minute | 5-minute }  Enable/disable logging to hard disk and then uploading to FortiAnalyzer.
    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.
  set upload-interval { daily | weekly | monthly }  Frequency to upload log files to FortiAnalyzer.
    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.
  set upload-day { string }  Day of week (month) to upload logs.
  set upload-time { string }  Time to upload logs (hh:mm).
```

```
set reliable { enable | disable } Enable/disable reliable logging to FortiAnalyzer.  
end
```

log {fortianalyzer | fortianalyzer2 | fortianalyzer3} filter

Introduction.



The exact same entries can be found under the `fortianalyzer`, `fortianalyzer2`, and `fortianalyzer3` filter commands.

```
config log fortianalyzer filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dlp-archive { enable | disable }  Enable/disable DLP archive logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  FortiAnalyzer log filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```

log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting

Introduction.



The exact same entries can be found under the `fortianalyzer`, `fortianalyzer2`, and `fortianalyzer3` setting commands.

```
config log fortianalyzer setting
  set status { enable | disable } Enable/disable logging to FortiAnalyzer.
  set ips-archive { enable | disable } Enable/disable IPS packet archive logging.
  set server { string } IPv4 or IPv6 address of the remote FortiAnalyzer. size[63]
  set hmac-algorithm { sha256 | sha1 } FortiAnalyzer IPsec tunnel HMAC algorithm.
    sha256 Use SHA256 as HMAC algorithm.
    sha1 Step down to SHA1 as the HMAC algorithm.
  set enc-algorithm { high-medium | high | low | disable } Enable/disable sending FortiAnalyzer log data with SSL encryption.
    high-medium Encrypt logs using high and medium encryption algorithm.
    high Encrypt logs using high encryption algorithm.
    low Encrypt logs using low encryption algorithm.
    disable Disable SSL encryption.
  set conn-timeout { integer } FortiAnalyzer connection time-out in seconds (for status and log buffer). range[1-3600]
  set monitor-keepalive-period { integer } Time between OFTP keepalives in seconds (for status and log buffer). range[1-120]
  set monitor-failure-retry-period { integer } Time between FortiAnalyzer connection retries in seconds (for status and log buffer). range[1-86400]
  set mgmt-name { string } Hidden management name of FortiAnalyzer. size[35]
  set faz-type { integer } Hidden setting index of FortiAnalyzer. range[0-4294967295]
  set certificate { string } Certificate used to communicate with FortiAnalyzer. size[35] - datasource(s): certificate.local.name
  set source-ip { string } Source IPv4 or IPv6 address used to communicate with FortiAnalyzer. size[63]
  set __change_ip { integer } Hidden attribute. range[0-255]
  set upload-option { store-and-upload | realtime | 1-minute | 5-minute } Enable/disable logging to hard disk and then uploading to FortiAnalyzer.
    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.
  set upload-interval { daily | weekly | monthly } Frequency to upload log files to FortiAnalyzer.
    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.
set upload-day { string } Day of week (month) to upload logs.
set upload-time { string } Time to upload logs (hh:mm).
set reliable { enable | disable } Enable/disable reliable logging to FortiAnalyzer.
end
```

log fortiguard filter

Introduction.

```
config log fortiguard filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dlp-archive { enable | disable }  Enable/disable DLP archive logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  FortiCloud log filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```

log fortiguard override-filter

Introduction.

```
config log fortiguard override-filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dlp-archive { enable | disable }  Enable/disable DLP archive logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  FortiCloud log filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```


log fortiguard override-setting

Introduction.

```
config log fortiguard override-setting
  set override { enable | disable }  Overriding FortiCloud settings for this VDOM or use global settings.
  set status { enable | disable }  Enable/disable logging to FortiCloud.
  set upload-option { store-and-upload | realtime | 1-minute | 5-minute }  Configure how log messages are sent to FortiCloud.
    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.
  set upload-interval { daily | weekly | monthly }  Frequency of uploading log files to FortiCloud.
    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.
  set upload-day { string }  Day of week to roll logs.
  set upload-time { string }  Time of day to roll logs (hh:mm).
end
```

log fortiguard setting

Introduction.

```
config log fortiguard setting
  set status { enable | disable }  Enable/disable logging to FortiCloud.
  set upload-option { store-and-upload | realtime | 1-minute | 5-minute }  Configure how log messages are sent to FortiCloud.
    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.
  set upload-interval { daily | weekly | monthly }  Frequency of uploading log files to FortiCloud.
    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.
  set upload-day { string }  Day of week to roll logs.
  set upload-time { string }  Time of day to roll logs (hh:mm).
  set enc-algorithm { high-medium | high | low | disable }  Enable/disable and set the SSL security level for for sending encrypted logs to
FortiCloud.
    high-medium  Encrypt logs using high and medium encryption.
    high         Encrypt logs using high encryption.
    low          Encrypt logs using low encryption.
    disable      Disable SSL encryption.
  set source-ip { ipv4 address }  Source IP address used to connect FortiCloud.
end
```

log gui-display

Use `log gui-display` to customize which logging content is visible in the GUI.

```
config log gui-display
  set resolve-hosts { enable | disable }  Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup
  set resolve-apps { enable | disable }   Resolve unknown applications on the GUI using Fortinet's remote application database.
  set fortiview-uncscanned-apps { enable | disable }  Enable/disable showing unscanned traffic in FortiView application charts.
  set location { memory | disk | fortianalyzer | forticloud }  Configure the GUI to show memory logs, disk logs, FortiAnalyzer logs, or FortiCloud logs.
  memory          Display memory logs on the GUI.
  disk            Display disk logs on the GUI.
  fortianalyzer   Display FortiAnalyzer logs on the GUI.
  forticloud      Display FortiCloud logs on the GUI.
end
```

resolve-hosts {enable | disable}

If enabled, Log & Report GUI pages will display resolved hostnames using reverse DNS lookup.

resolve-apps {enable | disable}

If enabled, the FortiGate will search the Internet Service Database to resolve unknown applications in traffic logs.

fortiview-uncscanned-apps {enable | disable}

Determines whether FortiView will display unscanned applications or not.

fortiview-local-traffic {enable | disable}

Determines whether FortiView will display local traffic logs.

location {memory | disk | fortianalyzer | fortiguard}

This command allows you to select which location's logs are visible in the GUI:

- `memory`: GUI will display memory logs.
- `disk`: GUI will display disk logs.
- `fortianalyzer`: GUI will display logs from FortiAnalyzer.
- `fortiguard`: GUI will display logs from FortiCloud.

log memory filter

Introduction.

```
config log memory filter
  set severity { option } Log every message above and including this severity level.
    emergency Emergency level.
    alert Alert level.
    critical Critical level.
    error Error level.
    warning Warning level.
    notification Notification level.
    information Information level.
    debug Debug level.
  set forward-traffic { enable | disable } Enable/disable forward traffic logging.
  set local-traffic { enable | disable } Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable } Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable } Enable/disable sniffer traffic logging.
  set anomaly { enable | disable } Enable/disable anomaly logging.
  set voip { enable | disable } Enable/disable VoIP logging.
  set dns { enable | disable } Enable/disable detailed DNS event logging.
  set event { enable | disable } Enable/disable event logging.
  set system { enable | disable } Enable/disable system activity logging.
  set radius { enable | disable } Enable/disable RADIUS messages logging.
  set ipsec { enable | disable } Enable/disable IPsec negotiation messages logging.
  set dhcp { enable | disable } Enable/disable DHCP service messages logging.
  set ppp { enable | disable } Enable/disable L2TP/PPTP/PPPoE logging.
  set admin { enable | disable } Enable/disable admin login/logout logging.
  set ha { enable | disable } Enable/disable HA logging.
  set auth { enable | disable } Enable/disable firewall authentication logging.
  set pattern { enable | disable } Enable/disable pattern update logging.
  set sslvpn-log-auth { enable | disable } Enable/disable SSL user authentication logging.
  set sslvpn-log-adm { enable | disable } Enable/disable SSL administrator login logging.
  set sslvpn-log-session { enable | disable } Enable/disable SSL session logging.
  set vip-ssl { enable | disable } Enable/disable VIP SSL logging.
  set ldb-monitor { enable | disable } Enable/disable VIP real server health monitoring logging.
  set wan-opt { enable | disable } Enable/disable WAN optimization eventlogging.
  set wireless-activity { enable | disable } Enable/disable wireless activity event logging.
  set cpu-memory-usage { enable | disable } Enable/disable CPU & memory usage logging every 5 minutes.
```

```
set filter { string } Memory log filter. size[511]
set filter-type { include | exclude } Include/exclude logs that match the filter.
    include Include logs that match the filter.
    exclude Exclude logs that match the filter.
end
```

log memory global-setting

Introduction.

```
config log memory global-setting
  set max-size { integer }    Maximum amount of memory that can be used for memory logging in bytes. range[0-4294967295]
  set full-first-warning-threshold { integer }  Log full first warning threshold as a percent (1 - 98, default = 75). range[1-98]
  set full-second-warning-threshold { integer }  Log full second warning threshold as a percent (2 - 99, default = 90). range[2-99]
  set full-final-warning-threshold { integer }  Log full final warning threshold as a percent (3 - 100, default = 95). range[3-100]
end
```

log memory setting

Introduction.

```
config log memory setting
  set status { enable | disable }  Enable/disable logging to the FortiGate's memory.
  set diskfull { overwrite }  Action to take when memory is full.
    overwrite Overwrite the oldest logs when the system memory reserved for logging is full.
end
```


log null-device filter

Introduction.

```
config log null-device filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  Null-device log filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```

log null-device setting

Introduction.

```
config log null-device setting
    set status { enable | disable }  Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is
present (data is not saved).
end
```

log setting

Introduction.

```
config log setting
  set resolve-ip { enable | disable }  Enable/disable adding resolved domain names to traffic logs if possible.
  set resolve-port { enable | disable }  Enable/disable adding resolved service names to traffic logs.
  set log-user-in-upper { enable | disable }  Enable/disable logs with user-in-upper.
  set fwpolicy-implicit-log { enable | disable }  Enable/disable implicit firewall policy logging.
  set fwpolicy6-implicit-log { enable | disable }  Enable/disable implicit firewall policy6 logging.
  set log-invalid-packet { enable | disable }  Enable/disable invalid packet traffic logging.
  set local-in-allow { enable | disable }  Enable/disable local-in-allow logging.
  set local-in-deny-unicast { enable | disable }  Enable/disable local-in-deny-unicast logging.
  set local-in-deny-broadcast { enable | disable }  Enable/disable local-in-deny-broadcast logging.
  set local-out { enable | disable }  Enable/disable local-out logging.
  set daemon-log { enable | disable }  Enable/disable daemon logging.
  set neighbor-event { enable | disable }  Enable/disable neighbor event logging.
  set brief-traffic-format { enable | disable }  Enable/disable brief format traffic logging.
  set user-anonymize { enable | disable }  Enable/disable anonymizing user names in log messages.
  set fortiview-weekly-data { enable | disable }  Enable/disable FortiView weekly data.
  set expolicy-implicit-log { enable | disable }  Enable/disable explicit proxy firewall implicit policy logging.
  set log-policy-comment { enable | disable }  Enable/disable inserting policy comments into traffic logs.
end
```

log syslogd override-filter

Introduction.

```
config log syslogd override-filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  Syslog filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```

log syslogd override-setting

Introduction.

```
config log syslogd override-setting
  set override { enable | disable }  Enable/disable override syslog settings.
  set status { enable | disable }  Enable/disable remote syslog logging.
  set server { string }  Address of remote syslog server. size[63]
  set reliable { enable | disable }  Enable/disable reliable logging (RFC3195).
  set port { integer }  Server listen port. range[0-65535]
  set facility { option }  Remote syslog facility.
    kernel  Kernel messages.
    user    Random user-level messages.
    mail    Mail system.
    daemon  System daemons.
    auth    Security/authorization messages.
    syslog  Messages generated internally by syslog.
    lpr     Line printer subsystem.
    news    Network news subsystem.
    uucp    Network news subsystem.
    cron    Clock daemon.
    authpriv Security/authorization messages (private).
    ftp     FTP daemon.
    ntp     NTP daemon.
    audit   Log audit.
    alert   Log alert.
    clock   Clock daemon.
    local0  Reserved for local use.
    local1  Reserved for local use.
    local2  Reserved for local use.
    local3  Reserved for local use.
    local4  Reserved for local use.
    local5  Reserved for local use.
    local6  Reserved for local use.
    local7  Reserved for local use.
  set source-ip { string }  Source IP address of syslog. size[63]
  set format { default | csv | cef }  Log format.
    default Syslog format.
    csv     CSV (Comma Separated Values) format.
```

```
        cef      CEF (Common Event Format) format.
config custom-field-name
  edit { id }
    # Custom field name for CEF format logging.
    set id { integer }  Entry ID. range[0-255]
    set name { string }  Field name. size[35]
    set custom { string }  Field custom name. size[35]
  next
end
```

log {syslogd | syslogd2 | syslogd3 | syslogd4} filter

Introduction.



The exact same entries can be found under the `syslogd`, `syslogd2`, `syslogd3`, and `syslogd4` filter commands.

```
config log syslogd filter
  set severity { option }  Lowest severity level to log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  Syslog filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```

log {syslogd | syslogd2 | syslogd3 | syslogd4} setting

Introduction.



The exact same entries can be found under the `syslogd`, `syslogd2`, `syslogd3`, and `syslogd4` setting commands.

```
config log syslogd setting
  set status { enable | disable }  Enable/disable remote syslog logging.
  set server { string }  Address of remote syslog server. size[63]
  set reliable { enable | disable }  Enable/disable reliable logging (RFC3195).
  set port { integer }  Server listen port. range[0-65535]
  set facility { option }  Remote syslog facility.
    kernel  Kernel messages.
    user    Random user-level messages.
    mail    Mail system.
    daemon  System daemons.
    auth    Security/authorization messages.
    syslog  Messages generated internally by syslog.
    lpr     Line printer subsystem.
    news    Network news subsystem.
    uucp    Network news subsystem.
    cron    Clock daemon.
    authpriv Security/authorization messages (private).
    ftp     FTP daemon.
    ntp     NTP daemon.
    audit   Log audit.
    alert   Log alert.
    clock   Clock daemon.
    local0  Reserved for local use.
    local1  Reserved for local use.
    local2  Reserved for local use.
    local3  Reserved for local use.
    local4  Reserved for local use.
    local5  Reserved for local use.
    local6  Reserved for local use.
```



```
    local7    Reserved for local use.
set source-ip { string }  Source IP address of syslog. size[63]
set format { default | csv | cef }  Log format.
    default  Syslog format.
    csv      CSV (Comma Separated Values) format.
    cef      CEF (Common Event Format) format.
config custom-field-name
    edit { id }
    # Custom field name for CEF format logging.
    set id { integer }  Entry ID. range[0-255]
    set name { string }  Field name. size[35]
    set custom { string }  Field custom name. size[35]
    next
end
```

log threat-weight

Use `log threat-weight` to enable and customize the threat-weight feature, which assigns logs a threat score based on configurable factors.

Note: `status` must be enabled for the rest of the options to be available.

```
config log threat-weight
  set status { enable | disable }  Enable/disable the threat weight feature.
  set low { integer }  Low level score value (1 - 100). range[1-100]
  set medium { integer }  Medium level score value (1 - 100). range[1-100]
  set high { integer }  High level score value (1 - 100). range[1-100]
  set critical { integer }  Critical level score value (1 - 100). range[1-100]
  set blocked-connection { option }  Threat weight score for blocked connections.
    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.
  set failed-connection { option }  Threat weight score for failed connections.
    disable  Disable threat weight scoring for failed connections.
    low      Use the low level score for failed connections.
    medium   Use the medium level score for failed connections.
    high     Use the high level score for failed connections.
    critical Use the critical level score for failed connections.
  set malware-detected { option }  Threat weight score for detected malware.
    disable  Disable threat weight scoring for detected malware.
    low      Use the low level score for detected malware.
    medium   Use the medium level score for detected malware.
    high     Use the high level score for detected malware.
    critical Use the critical level score for detected malware.
  set url-block-detected { option }  Threat weight score for URL blocking.
    disable  Disable threat weight scoring for URL blocking.
    low      Use the low level score for URL blocking.
    medium   Use the medium level score for URL blocking.
    high     Use the high level score for URL blocking.
    critical Use the critical level score for URL blocking.
  set botnet-connection-detected { option }  Threat weight score for detected botnet connections.
    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.
set info-severity { option } Threat weight score for IPS info severity events.
    disable  Disable threat weight scoring for IPS info severity events.
    low      Use the low level score for IPS info severity events.
    medium   Use the medium level score for IPS info severity events.
    high     Use the high level score for IPS info severity events.
    critical Use the critical level score for IPS info severity events.
set low-severity { option } Threat weight score for IPS low severity events.
    disable  Disable threat weight scoring for IPS low severity events.
    low      Use the low level score for IPS low severity events.
    medium   Use the medium level score for IPS low severity events.
    high     Use the high level score for IPS low severity events.
    critical Use the critical level score for IPS low severity events.
set medium-severity { option } Threat weight score for IPS medium severity events.
    disable  Disable threat weight scoring for IPS medium severity events.
    low      Use the low level score for IPS medium severity events.
    medium   Use the medium level score for IPS medium severity events.
    high     Use the high level score for IPS medium severity events.
    critical Use the critical level score for IPS medium severity events.
set high-severity { option } Threat weight score for IPS high severity events.
    disable  Disable threat weight scoring for IPS high severity events.
    low      Use the low level score for IPS high severity events.
    medium   Use the medium level score for IPS high severity events.
    high     Use the high level score for IPS high severity events.
    critical Use the critical level score for IPS high severity events.
set critical-severity { option } Threat weight score for IPS critical severity events.
    disable  Disable threat weight scoring for IPS critical severity events.
    low      Use the low level score for IPS critical severity events.
    medium   Use the medium level score for IPS critical severity events.
    high     Use the high level score for IPS critical severity events.
    critical Use the critical level score for IPS critical severity events.
config web
edit { id }
# Web filtering threat weight settings.
set id { integer } Entry ID. range[0-255]
set category { integer } Threat weight score for web category filtering matches. range[0-255]
set level { option } Threat weight score for web category filtering matches.
    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.
    next
config geolocation
    edit { id }
    # Geolocation-based threat weight settings.
    set id { integer } Entry ID. range[0-255]
    set country { string } Country code. size[2]
    set level { option } Threat weight score for Geolocation-based events.
        disable Disable threat weight scoring for Geolocation-based events.
        low Use the low level score for Geolocation-based events.
        medium Use the medium level score for Geolocation-based events.
        high Use the high level score for Geolocation-based events.
        critical Use the critical level score for Geolocation-based events.
    next
config application
    edit { id }
    # Application-control threat weight settings.
    set id { integer } Entry ID. range[0-255]
    set category { integer } Application category. range[0-65535]
    set level { option } Threat weight score for Application events.
        disable Disable threat weight scoring for Application events.
        low Use the low level score for Application events.
        medium Use the medium level score for Application events.
        high Use the high level score for Application events.
        critical Use the critical level score for Application events.
    next
end
```

status {enable | disable}

Enable threat-weight calculation in logs.

config level

Use the below subcommands to set the scores for the four levels of threats.

- edit low <value>
- edit medium <value>

- `edit high <value>`
- `edit critical <value>`

blocked-connection {disable | low | medium | high | critical}

Set the threat-weight score for blocked-connection errors. `disable` assigns no score.

failed-connection {disable | low | medium | high | critical}

Set the threat-weight score for failed-connection errors. `disable` assigns no score.

malware-detected {disable | low | medium | high | critical}

Set the threat-weight score for malware detection in logs. `disable` assigns no score.

url-block-detected {disable | low | medium | high | critical}

Set the threat-weight score for URL blocking events. `disable` assigns no score.

botnet-connection-detected {disable | low | medium | high | critical}

Set the threat-weight score for botnet connection detections in logs. `disable` assigns no score.

config ips

Use the following subcommands to set the threat score assigned to IPS events at different severity levels:

- `set info-severity {disable | low | medium | high | critical}`
- `set low-severity {disable | low | medium | high | critical}`
- `set medium-severity {disable | low | medium | high | critical}`
- `set high-severity {disable | low | medium | high | critical}`
- `set critical-severity {disable | low | medium | high | critical}`

config web

Specific FortiGuard Web Filtering Categories that might appear in logs can be assigned a threat score, using the below commands:

edit <id>

A table value for custom threat score assignments for Categories. Edit to create new and configure the custom assignments using the following commands:

category <value>

The Category that will have a threat score assigned to it. You can view a list of Categories by entering `set category ?`.

level {disable | low | medium | high | critical}

The threat score assigned to the Web Filtering Category.

config geolocation

Specific geographic locations that might appear in logs can be assigned a threat score, using the below commands:

edit <id>

A table value for custom threat score assignments for countries. Edit to create new and configure the custom assignments using the following commands:

country <country code>

The country that will have a threat score assigned to it. You can view a list of country codes by entering `set country ?`.

level {disable | low | medium | high | critical}

The threat score assigned to the country.

config application

Specific FortiGuard Application categories that might appear in logs can be assigned a threat score, using the below commands:

edit <id>

A table value for custom threat score assignments for categories. Edit to create new and configure the custom assignments using the following commands:

category <value>

The application category that will have a threat score assigned to it. You can view a list of categories by entering `set category ?`.

level {disable | low | medium | high | critical}

The threat score assigned to the Application category.

log webtrends filter

Introduction.

```
config log webtrends filter
  set severity { option }  Lowest severity level to log to WebTrends.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
  set forward-traffic { enable | disable }  Enable/disable forward traffic logging.
  set local-traffic { enable | disable }  Enable/disable local in or out traffic logging.
  set multicast-traffic { enable | disable }  Enable/disable multicast traffic logging.
  set sniffer-traffic { enable | disable }  Enable/disable sniffer traffic logging.
  set anomaly { enable | disable }  Enable/disable anomaly logging.
  set voip { enable | disable }  Enable/disable VoIP logging.
  set dns { enable | disable }  Enable/disable detailed DNS event logging.
  set filter { string }  Webtrends log filter. size[511]
  set filter-type { include | exclude }  Include/exclude logs that match the filter.
    include  Include logs that match the filter.
    exclude  Exclude logs that match the filter.
end
```


log webtrends setting

Introduction.

```
config log webtrends setting
    set status { enable | disable }  Enable/disable logging to WebTrends.
    set server { string }  Address of the remote WebTrends server. size[63]
end
```

report

Introduction.

This section includes syntax for the following commands:

- [report chart](#)
- [report dataset](#)
- [report layout](#)
- [report setting](#)
- [report style](#)
- [report theme](#)

report chart

Introduction.

```
config report chart
  edit { name }
  # Report chart widget configuration.
  set name { string }  Chart Widget Name size[71]
  set policy { integer }  Used by monitor policy. range[0-4294967295]
  set type { graph | table }  Chart type.
    graph Graph.
    table Table.
  set period { last24h | last7d }  Time period.
    last24h Last 24 hours.
    last7d Last 7 days.
  config drill-down-charts
    edit { id }
    # Drill down charts.
    set id { integer }  Drill down chart ID. range[0-4294967295]
    set chart-name { string }  Drill down chart name. size[71]
    set status { enable | disable }  Enable/disable this drill down chart.
  next
  set comments { string }  Comment. size[127]
  set dataset { string }  Bind dataset to chart. size[71]
  set category { option }  Category.
    misc      Miscellaneous.
    traffic   Traffic.
    event     Event.
    virus     Virus.
    webfilter Webfilter.
    attack    Attack.
    spam      Spam.
    dlp       Data leak prevention.
    app-ctrl  Application control.
    vulnerability Vulnerability.
  set favorite { no | yes }  Favorite.
    no  Not a favorite chart.
    yes Favorite chart.
  set graph-type { option }  Graph type.
```

```

    none None.
    bar Bar Chart.
    pie Pie Chart.
    line Line Chart.
    flow flow Chart.
set style { auto | manual } Style.
    auto Auto.
    manual Manual.
set dimension { 2D | 3D } Dimension.
    2D 2D graphic.
    3D 3D graphic.
set databind { string } X-series value expression. size[127]
set caption { string } X-series caption. size[35]
set caption-font-size { integer } X-series caption font size. range[5-20]
set font-size { integer } X-series label font size. range[5-20]
set label-angle { 45-degree | vertical | horizontal } X-series label angle.
    45-degree 45-degree.
    vertical Vertical.
    horizontal Horizontal.
set is-category { yes | no } X-series represent category or not.
    yes X-series is category.
    no X-series is not category.
set scale-unit { option } Scale unit.
    minute Minute.
    hour Hour.
    day Day.
    month Month.
    year Year.
set scale-step { integer } Scale step. range[1-65535]
set scale-direction { decrease | increase } Scale increase or decrease.
    decrease Decrease.
    increase Increase.
set scale-format { option } Date/time format.
    YYYY-MM-DD-HH-MM YYYY/MM/DD HH:MM
    YYYY-MM-DD HH YYYY/MM/DD HH
    YYYY-MM-DD YYYY/MM/DD
    YYYY-MM YYYY/MM
    YYYY YYYY
    HH-MM HH:MM
    MM-DD MM:DD
set unit { string } X-series unit. size[35]
set databind { string } Y-series value expression. size[127]
set caption { string } Y-series caption. size[35]

```

```

set caption-font-size { integer } Y-series caption font size. range[5-20]
set font-size { integer } Y-series label font size. range[5-20]
set label-angle { 45-degree | vertical | horizontal } Y-series label angle.
    45-degree 45-degree.
    vertical Vertical.
    horizontal Horizontal.
set group { string } Y-series group option. size[127]
set unit { string } Y-series unit. size[35]
set extra-y { enable | disable } Allow another Y-series value
set extra-databind { string } Extra Y-series value. size[127]
set y-legend { string } First Y-series legend type/name. size[35]
set extra-y-legend { string } Extra Y-series legend type/name. size[35]
set databind { string } Category series value expression. size[127]
set font-size { integer } Font size of category-series title. range[5-20]
set databind { string } Value series value expression. size[127]
set title { string } Chart title. size[63]
set title-font-size { integer } Font size of chart title. range[0-4294967295]
set background { string } Chart background. size[11]
set color-palette { string } Color palette (system will pick color automatically by default). size[11]
set legend { enable | disable } Enable/Disable Legend area.
set legend-font-size { integer } Font size of legend area. range[0-4294967295]
config column
edit { id }
# Table column definition.
set id { integer } ID. range[0-4294967295]
set header-value { string } Display name of table header. size[127]
set detail-value { string } Detail value of column. size[127]
set footer-value { string } Footer value of column. size[127]
set detail-unit { string } Detail unit of column. size[35]
set footer-unit { string } Footer unit of column. size[35]
config mapping
edit { id }
# Show detail in certain display value for certain condition.
set id { integer } id range[0-4294967295]
set op { option } Comparison operator.
    none None.
    greater Greater than.
    greater-equal Greater than or equal to.
    less Less than.
    less-equal Less than or equal to.
    equal Equal to.
    between Between value 1 and value 2.
set value-type { integer | string } Value type.

```

```
        integer Integer.
        string String.
    set value1 { string } Value 1. size[127]
    set value2 { string } Value 2. size[127]
    set displayname { string } Display name. size[127]
next
next
next
end
```

report dataset

Introduction.

```
config report dataset
  edit { name }
  # Report dataset configuration.
  set name { string } Name. size[71]
  set policy { integer } Used by monitor policy. range[0-4294967295]
  set query { string } SQL query statement. size[2047]
  config field
    edit { id }
    # Fields.
    set id { integer } Field ID (1 to number of columns in SQL result). range[0-4294967295]
    set type { text | integer | double } Field type.
      text Text.
      integer Integer.
      double Double.
    set name { string } Name. size[71]
    set displayname { string } Display name. size[127]
  next
  config parameters
    edit { id }
    # Parameters.
    set id { integer } Parameter ID (1 to number of columns in SQL result). range[0-4294967295]
    set display-name { string } Display name. size[127]
    set field { string } SQL field name. size[127]
    set data-type { option } Data type.
      text Text.
      integer Integer.
      double Double.
      long-integer Long integer.
      date-time Date and time.
  next
next
end
```

report layout

Introduction.

```
config report layout
edit { name }
# Report layout configuration.
set name { string } Report layout name. size[35]
set title { string } Report title. size[127]
set subtitle { string } Report subtitle. size[127]
set description { string } Description. size[127]
set style-theme { string } Report style theme. size[35]
set options { option } Report layout options.
    include-table-of-content Include table of content in the report.
    auto-numbering-heading Prepend heading with auto numbering.
    view-chart-as-heading Auto add heading for each chart.
    show-html-navbar-before-heading Show HTML navigation bar before each heading.
    dummy-option Use this option if you need none of the above options.
set format { pdf } Report format.
    pdf PDF.
set schedule-type { demand | daily | weekly } Report schedule type.
    demand Run on demand.
    daily Schedule daily.
    weekly Schedule weekly.
set day { option } Schedule days of week to generate report.
    sunday Sunday.
    monday Monday.
    tuesday Tuesday.
    wednesday Wednesday.
    thursday Thursday.
    friday Friday.
    saturday Saturday.
set time { string } Schedule time to generate report [hh:mm].
set cutoff-option { run-time | custom } Cutoff-option is either run-time or custom.
    run-time Run time.
    custom Custom.
set cutoff-time { string } Custom cutoff time to generate report [hh:mm].
set email-send { enable | disable } Enable/disable sending emails after reports are generated.
set email-recipients { string } Email recipients for generated reports. size[511]
```



```
set max-pdf-report { integer } Maximum number of PDF reports to keep at one time (oldest report is overwritten). range[1-365]
set paper { a4 | letter } Report page paper.
    a4      A4 paper.
    letter Letter paper.
set column-break-before { heading1 | heading2 | heading3 } Report page auto column break before heading.
    heading1 Column break before heading 1.
    heading2 Column break before heading 2.
    heading3 Column break before heading 3.
set page-break-before { heading1 | heading2 | heading3 } Report page auto page break before heading.
    heading1 Page break before heading 1.
    heading2 Page break before heading 2.
    heading3 Page break before heading 3.
set options { header-on-first-page | footer-on-first-page } Report page options.
    header-on-first-page Show header on first page.
    footer-on-first-page Show footer on first page.
set style { string } Report header style. size[71]
config header-item
    edit { id }
    # Configure report header item.
        set id { integer } Report item ID. range[0-4294967295]
        set description { string } Description. size[63]
        set type { text | image } Report item type.
            text Text.
            image Image.
        set style { string } Report item style. size[71]
        set content { string } Report item text content. size[511]
        set img-src { string } Report item image file name. size[127]
    next
set style { string } Report footer style. size[71]
config footer-item
    edit { id }
    # Configure report footer item.
        set id { integer } Report item ID. range[0-4294967295]
        set description { string } Description. size[63]
        set type { text | image } Report item type.
            text Text.
            image Image.
        set style { string } Report item style. size[71]
        set content { string } Report item text content. size[511]
        set img-src { string } Report item image file name. size[127]
    next
config body-item
    edit { id }
```

```
# Configure report body item.
set id { integer } Report item ID. range[0-4294967295]
set description { string } Description. size[63]
set type { text | image | chart | misc } Report item type.
    text Text.
    image Image.
    chart Chart.
    misc Miscellaneous.
set style { string } Report item style. size[71]
set top-n { integer } Value of top. range[0-4294967295]
set hide { enable | disable } Enable/disable hide item in report.
config parameters
    edit { id }
        # Parameters.
        set id { integer } ID. range[0-4294967295]
        set name { string } Field name that match field of parameters defined in dataset. size[127]
        set value { string } Value to replace corresponding field of parameters defined in dataset. size[1023]
    next
set text-component { text | heading1 | heading2 | heading3 } Report item text component.
    text Normal text.
    heading1 Heading 1.
    heading2 Heading 2.
    heading3 Heading 3.
set content { string } Report item text content. size[511]
set img-src { string } Report item image file name. size[127]
set list-component { bullet | numbered } Report item list component.
    bullet Bullet list.
    numbered Numbered list.
config list
    edit { id }
        # Configure report list item.
        set id { integer } List entry ID. range[0-4294967295]
        set content { string } List entry content. size[127]
    next
set chart { string } Report item chart name. size[71]
set chart-options { include-no-data | hide-title | show-caption } Report chart options.
    include-no-data Include chart with no data.
    hide-title Hide chart title.
    show-caption Show chart caption.
set drill-down-items { string } Control how drill down charts are shown. size[11]
set drill-down-types { string } Control whether keys from the parent being combined or not. size[7]
set table-column-widths { string } Report item table column widths. size[179]
set table-caption-style { string } Table chart caption style. size[71]
```

```
set table-head-style { string } Table chart head style. size[71]
set table-odd-row-style { string } Table chart odd row style. size[71]
set table-even-row-style { string } Table chart even row style. size[71]
set misc-component { hline | page-break | column-break | section-start } Report item miscellaneous component.
    hline Horizontal line.
    page-break Page break.
    column-break Column break.
    section-start Section start.
set column { integer } Report section column number. range[0-4294967295]
set title { string } Report section title. size[511]
next
end
```

report setting

Introduction.

```
config report setting
  set pdf-report { enable | disable }  Enable/disable PDF report.
  set fortiview { enable | disable }  Enable/disable historical FortiView.
  set report-source { forward-traffic | sniffer-traffic | local-deny-traffic }  Report log source.
    forward-traffic  Report includes forward traffic logs.
    sniffer-traffic  Report includes sniffer traffic logs.
    local-deny-traffic  Report includes local deny traffic logs.
  set web-browsing-threshold { integer }  Web browsing time calculation threshold (3 - 15 min). range[3-15]
end
```

report style

Introduction.

```
config report style
  edit { name }
  # Report style configuration.
  set name { string } Report style name. size[71]
  set options { option } Report style options.
    font Font.
    text Text.
    color Color.
    align Align.
    size Size.
    margin Margin.
    border Border.
    padding Padding.
    column Column.
  set font-family { option } Font family.
    Verdana Verdana.
    Arial Arial.
    Helvetica Helvetica.
    Courier Courier.
    Times Times Roman.
  set font-style { normal | italic } Font style.
    normal Normal.
    italic Italic.
  set font-weight { normal | bold } Font weight.
    normal Normal.
    bold Bold.
  set font-size { string } Font size. size[15]
  set line-height { string } Text line height. size[15]
  set fg-color { string } Foreground color. size[15]
  set bg-color { string } Background color. size[15]
  set align { left | center | right | justify } Alignment.
    left Align left.
    center Align center.
    right Align right.
    justify Align justify.
```

```
set width { string } Width. size[15]
set height { string } Height. size[15]
set margin-top { string } Margin top. size[15]
set margin-right { string } Margin right. size[15]
set margin-bottom { string } Margin bottom. size[15]
set margin-left { string } Margin left. size[15]
set border-top { string } Border top.
set border-right { string } Border right.
set border-bottom { string } Border bottom.
set border-left { string } Border left.
set padding-top { string } Padding top. size[15]
set padding-right { string } Padding right. size[15]
set padding-bottom { string } Padding bottom. size[15]
set padding-left { string } Padding left. size[15]
set column-span { none | all } Column span.
    none Does not span.
    all Span across all columns.
set column-gap { string } Column gap. size[15]
next
end
```

report theme

Introduction.

```
config report theme
  edit { name }
  # Report themes configuration
  set name { string } Report theme name. size[35]
  set page-orient { portrait | landscape } Report page orientation.
    portrait Portrait Orientation.
    landscape Landscape Orientation.
  set column-count { 1 | 2 | 3 } Report page column count.
    1 One Column.
    2 Two Columns.
    3 Three Columns.
  set default-html-style { string } Default HTML report style. size[71]
  set default-pdf-style { string } Default PDF report style. size[71]
  set page-style { string } Report page style. size[71]
  set page-header-style { string } Report page header style. size[71]
  set page-footer-style { string } Report page footer style. size[71]
  set report-title-style { string } Report title style. size[71]
  set report-subtitle-style { string } Report subtitle style. size[71]
  set toc-title-style { string } Table of contents title style. size[71]
  set toc-heading1-style { string } Table of contents heading style. size[71]
  set toc-heading2-style { string } Table of contents heading style. size[71]
  set toc-heading3-style { string } Table of contents heading style. size[71]
  set toc-heading4-style { string } Table of contents heading style. size[71]
  set heading1-style { string } Report heading style. size[71]
  set heading2-style { string } Report heading style. size[71]
  set heading3-style { string } Report heading style. size[71]
  set heading4-style { string } Report heading style. size[71]
  set normal-text-style { string } Normal text style. size[71]
  set bullet-list-style { string } Bullet list style. size[71]
  set numbered-list-style { string } Numbered list style. size[71]
  set image-style { string } Image style. size[71]
  set hline-style { string } Horizontal line style. size[71]
  set graph-chart-style { string } Graph chart style. size[71]
  set table-chart-style { string } Table chart style. size[71]
  set table-chart-caption-style { string } Table chart caption style. size[71]
```

```
set table-chart-head-style { string } Table chart head row style. size[71]
set table-chart-odd-row-style { string } Table chart odd row style. size[71]
set table-chart-even-row-style { string } Table chart even row style. size[71]
next
end
```


router

Introduction.

This section includes syntax for the following commands:

- `router access-list | access-list6`
- `router aspath-list`
- `router auth-path`
- `router bfd`
- `router bgp`
- `router community-list`
- `router isis`
- `router key-chain`
- `router multicast | multicast6`
- `router multicast-flow`
- `router ospf | ospf6`
- `router policy | policy6`
- `router prefix-list | prefix-list6`
- `router rip`
- `router ripng`
- `router route-map`
- `router setting`
- `router static | static6`

router {access-list | access-list6}

Introduction.

```
config router access-list
  edit { name }
  # Configure access lists.
  set name { string } Name. size[35]
  set comments { string } Comment. size[127]
  config rule
    edit { id }
    # Rule.
    set id { integer } Rule ID. range[0-4294967295]
    set action { permit | deny } Permit or deny this IP address and netmask prefix.
      permit Permit or allow this IP address and netmask prefix.
      deny Deny this IP address and netmask prefix.
    set prefix { string } IPv4 prefix to define regular filter criteria, such as "any" or subnets.
    set wildcard { string } Wildcard to define Cisco-style wildcard filter criteria.
    set exact-match { enable | disable } Enable/disable exact match.
    set flags { integer } Flags. range[0-4294967295]
  next
next
end

config router access-list6
  edit { name }
  # Configure IPv6 access lists.
  set name { string } Name. size[35]
  set comments { string } Comment. size[127]
  config rule
    edit { id }
    # Rule.
    set id { integer } Rule ID. range[0-4294967295]
    set action { permit | deny } Permit or deny this IP address and netmask prefix.
      permit Permit or allow this IP address and netmask prefix.
      deny Deny this IP address and netmask prefix.
    set prefix6 { string } IPv6 prefix to define regular filter criteria, such as "any" or subnets.
```

```
        set exact-match { enable | disable }  Enable/disable exact prefix match.
        set flags { integer }  Flags. range[0-4294967295]
    next
end
```

router aspath-list

Introduction.

```
config router aspath-list
  edit { name }
  # Configure Autonomous System (AS) path lists.
  set name { string } AS path list name. size[35]
  config rule
    edit { id }
    # AS path list rule.
    set id { integer } ID. range[0-4294967295]
    set action { deny | permit } Permit or deny route-based operations, based on the route's AS_PATH attribute.
      deny Deny route-based operations.
      permit Permit route-based operations.
    set regexp { string } Regular-expression to match the Border Gateway Protocol (BGP) AS paths. size[63]
  next
next
end
```

router auth-path

Introduction.

```
config router auth-path
  edit { name }
  # Configure authentication based routing.
  set name { string } Name of the entry. size[15]
  set device { string } Outgoing interface. size[35] - datasource(s): system.interface.name
  set gateway { ipv4 address } Gateway IP address.
next
end
```

router bfd

Introduction.

```
config router bfd
  config neighbor
    edit { ip }
    # neighbor
    set ip { ipv4 address }  IPv4 address of the BFD neighbor.
    set interface { string }  Interface name. size[15] - datasource(s): system.interface.name
  next
end
```

router bgp

Introduction.

```
config router bgp
  set as { integer } Router AS number, valid from 1 to 4294967295, 0 to disable BGP. range[0-4294967295]
  set router-id { ipv4 address any } Router ID.
  set keepalive-timer { integer } Frequency to send keep alive requests. range[0-65535]
  set holdtime-timer { integer } Number of seconds to mark peer as dead. range[3-65535]
  set always-compare-med { enable | disable } Enable/disable always compare MED.
  set bestpath-as-path-ignore { enable | disable } Enable/disable ignore AS path.
  set bestpath-cmp-confed-aspash { enable | disable } Enable/disable compare federation AS path length.
  set bestpath-cmp-routerid { enable | disable } Enable/disable compare router ID for identical EBGp paths.
  set bestpath-med-confed { enable | disable } Enable/disable compare MED among confederation paths.
  set bestpath-med-missing-as-worst { enable | disable } Enable/disable treat missing MED as least preferred.
  set client-to-client-reflection { enable | disable } Enable/disable client-to-client route reflection.
  set dampening { enable | disable } Enable/disable route-flap dampening.
  set deterministic-med { enable | disable } Enable/disable enforce deterministic comparison of MED.
  set ebgp-multipath { enable | disable } Enable/disable EBGp multi-path.
  set ibgp-multipath { enable | disable } Enable/disable IBGP multi-path.
  set enforce-first-as { enable | disable } Enable/disable enforce first AS for EBGp routes.
  set fast-external-failover { enable | disable } Enable/disable reset peer BGP session if link goes down.
  set log-neighbour-changes { enable | disable } Enable logging of BGP neighbour's changes
  set network-import-check { enable | disable } Enable/disable ensure BGP network route exists in IGP.
  set ignore-optional-capability { enable | disable } Don't send unknown optional capability notification message
  set cluster-id { ipv4 address any } Route reflector cluster ID.
  set confederation-identifier { integer } Confederation identifier. range[1-4294967295]
config confederation-peers
  edit { peer }
  # Confederation peers.
  set peer { string } Peer ID. size[64]
  next
  set dampening-route-map { string } Criteria for dampening. size[35] - datasource(s): router.route-map.name
  set dampening-reachability-half-life { integer } Reachability half-life time for penalty (min). range[1-45]
  set dampening-reuse { integer } Threshold to reuse routes. range[1-20000]
  set dampening-suppress { integer } Threshold to suppress routes. range[1-20000]
  set dampening-max-suppress-time { integer } Maximum minutes a route can be suppressed. range[1-255]
  set dampening-unreachability-half-life { integer } Unreachability half-life time for penalty (min). range[1-45]
  set default-local-preference { integer } Default local preference. range[0-4294967295]
```

```
set scan-time { integer } Background scanner interval (sec), 0 to disable it. range[5-60]
set distance-external { integer } Distance for routes external to the AS. range[1-255]
set distance-internal { integer } Distance for routes internal to the AS. range[1-255]
set distance-local { integer } Distance for routes local to the AS. range[1-255]
set synchronization { enable | disable } Enable/disable only advertise routes from iBGP if routes present in an IGP.
set graceful-restart { enable | disable } Enable/disable BGP graceful restart capabilities.
set graceful-restart-time { integer } Time needed for neighbors to restart (sec). range[1-3600]
set graceful-stalepath-time { integer } Time to hold stale paths of restarting neighbor (sec). range[1-3600]
set graceful-update-delay { integer } Route advertisement/selection delay after restart (sec). range[1-3600]
set graceful-end-on-timer { enable | disable } Enable/disable to exit graceful restart on timer only.
config aggregate-address
  edit { id }
    # BGP aggregate address table.
    set id { integer } ID. range[0-4294967295]
    set prefix { ipv4 classnet any } Aggregate prefix.
    set as-set { enable | disable } Enable/disable generate AS set path information.
    set summary-only { enable | disable } Enable/disable filter more specific routes from updates.
  next
config aggregate-address6
  edit { id }
    # BGP IPv6 aggregate address table.
    set id { integer } ID. range[0-4294967295]
    set prefix6 { ipv6 prefix } Aggregate IPv6 prefix.
    set as-set { enable | disable } Enable/disable generate AS set path information.
    set summary-only { enable | disable } Enable/disable filter more specific routes from updates.
  next
config neighbor
  edit { ip }
    # BGP neighbor table.
    set ip { string } IP/IPv6 address of neighbor. size[45]
    set advertisement-interval { integer } Minimum interval (sec) between sending updates. range[1-600]
    set allowas-in-enable { enable | disable } Enable/disable IPv4 Enable to allow my AS in AS path.
    set allowas-in-enable6 { enable | disable } Enable/disable IPv6 Enable to allow my AS in AS path.
    set allowas-in { integer } IPv4 The maximum number of occurrence of my AS number allowed. range[1-10]
    set allowas-in6 { integer } IPv6 The maximum number of occurrence of my AS number allowed. range[1-10]
    set attribute-unchanged { as-path | med | next-hop } IPv4 List of attributes that should be unchanged.
      as-path AS path.
      med MED.
      next-hop Next hop.
    set attribute-unchanged6 { as-path | med | next-hop } IPv6 List of attributes that should be unchanged.
      as-path AS path.
      med MED.
      next-hop Next hop.
```



```

set activate { enable | disable } Enable/disable address family IPv4 for this neighbor.
set activate6 { enable | disable } Enable/disable address family IPv6 for this neighbor.
set bfd { enable | disable } Enable/disable BFD for this neighbor.
set capability-dynamic { enable | disable } Enable/disable advertise dynamic capability to this neighbor.
set capability-orf { none | receive | send | both } Accept/Send IPv4 ORF lists to/from this neighbor.
    none None.
    receive Receive ORF lists.
    send Send ORF list.
    both Send and receive ORF lists.
set capability-orf6 { none | receive | send | both } Accept/Send IPv6 ORF lists to/from this neighbor.
    none None.
    receive Receive ORF lists.
    send Send ORF list.
    both Send and receive ORF lists.
set capability-graceful-restart { enable | disable } Enable/disable advertise IPv4 graceful restart capability to this neighbor.
set capability-graceful-restart6 { enable | disable } Enable/disable advertise IPv6 graceful restart capability to this neighbor.
set capability-route-refresh { enable | disable } Enable/disable advertise route refresh capability to this neighbor.
set capability-default-originate { enable | disable } Enable/disable advertise default IPv4 route to this neighbor.
set capability-default-originate6 { enable | disable } Enable/disable advertise default IPv6 route to this neighbor.
set dont-capability-negotiate { enable | disable } Don't negotiate capabilities with this neighbor
set ebgp-enforce-multihop { enable | disable } Enable/disable allow multi-hop EBGp neighbors.
set link-down-failover { enable | disable } Enable/disable failover upon link down.
set stale-route { enable | disable } Enable/disable stale route after neighbor down.
set next-hop-self { enable | disable } Enable/disable IPv4 next-hop calculation for this neighbor.
set next-hop-self6 { enable | disable } Enable/disable IPv6 next-hop calculation for this neighbor.
set override-capability { enable | disable } Enable/disable override result of capability negotiation.
set passive { enable | disable } Enable/disable sending of open messages to this neighbor.
set remove-private-as { enable | disable } Enable/disable remove private AS number from IPv4 outbound updates.
set remove-private-as6 { enable | disable } Enable/disable remove private AS number from IPv6 outbound updates.
set route-reflector-client { enable | disable } Enable/disable IPv4 AS route reflector client.
set route-reflector-client6 { enable | disable } Enable/disable IPv6 AS route reflector client.
set route-server-client { enable | disable } Enable/disable IPv4 AS route server client.
set route-server-client6 { enable | disable } Enable/disable IPv6 AS route server client.
set shutdown { enable | disable } Enable/disable shutdown this neighbor.
set soft-reconfiguration { enable | disable } Enable/disable allow IPv4 inbound soft reconfiguration.
set soft-reconfiguration6 { enable | disable } Enable/disable allow IPv6 inbound soft reconfiguration.
set as-override { enable | disable } Enable/disable replace peer AS with own AS for IPv4.
set as-override6 { enable | disable } Enable/disable replace peer AS with own AS for IPv6.
set strict-capability-match { enable | disable } Enable/disable strict capability matching.
set default-originate-routemap { string } Route map to specify criteria to originate IPv4 default. size[35] - datasource(s): router-
.route-map.name
set default-originate-routemap6 { string } Route map to specify criteria to originate IPv6 default. size[35] - datasource(s): router-
.route-map.name

```

```

set description { string } Description. size[63]
set distribute-list-in { string } Filter for IPv4 updates from this neighbor. size[35] - datasource(s): router.access-list.name
set distribute-list-in6 { string } Filter for IPv6 updates from this neighbor. size[35] - datasource(s): router.access-list6.name
set distribute-list-out { string } Filter for IPv4 updates to this neighbor. size[35] - datasource(s): router.access-list.name
set distribute-list-out6 { string } Filter for IPv6 updates to this neighbor. size[35] - datasource(s): router.access-list6.name
set ebgp-multihop-ttl { integer } EBGp multihop TTL for this peer. range[1-255]
set filter-list-in { string } BGP filter for IPv4 inbound routes. size[35] - datasource(s): router.aspath-list.name
set filter-list-in6 { string } BGP filter for IPv6 inbound routes. size[35] - datasource(s): router.aspath-list.name
set filter-list-out { string } BGP filter for IPv4 outbound routes. size[35] - datasource(s): router.aspath-list.name
set filter-list-out6 { string } BGP filter for IPv6 outbound routes. size[35] - datasource(s): router.aspath-list.name
set interface { string } Interface size[15] - datasource(s): system.interface.name
set maximum-prefix { integer } Maximum number of IPv4 prefixes to accept from this peer. range[1-4294967295]
set maximum-prefix6 { integer } Maximum number of IPv6 prefixes to accept from this peer. range[1-4294967295]
set maximum-prefix-threshold { integer } Maximum IPv4 prefix threshold value (1 - 100 percent). range[1-100]
set maximum-prefix-threshold6 { integer } Maximum IPv6 prefix threshold value (1 - 100 percent). range[1-100]
set maximum-prefix-warning-only { enable | disable } Enable/disable IPv4 Only give warning message when limit is exceeded.
set maximum-prefix-warning-only6 { enable | disable } Enable/disable IPv6 Only give warning message when limit is exceeded.
set prefix-list-in { string } IPv4 Inbound filter for updates from this neighbor. size[35] - datasource(s): router.prefix-list.name
set prefix-list-in6 { string } IPv6 Inbound filter for updates from this neighbor. size[35] - datasource(s): router.prefix-list6.name
set prefix-list-out { string } IPv4 Outbound filter for updates to this neighbor. size[35] - datasource(s): router.prefix-list.name
set prefix-list-out6 { string } IPv6 Outbound filter for updates to this neighbor. size[35] - datasource(s): router.prefix-list6.name
set remote-as { integer } AS number of neighbor. range[1-4294967295]
set local-as { integer } Local AS number of neighbor. range[0-4294967295]
set local-as-no-prepend { enable | disable } Do not prepend local-as to incoming updates.
set local-as-replace-as { enable | disable } Replace real AS with local-as in outgoing updates.
set retain-stale-time { integer } Time to retain stale routes. range[0-65535]
set route-map-in { string } IPv4 Inbound route map filter. size[35] - datasource(s): router.route-map.name
set route-map-in6 { string } IPv6 Inbound route map filter. size[35] - datasource(s): router.route-map.name
set route-map-out { string } IPv4 Outbound route map filter. size[35] - datasource(s): router.route-map.name
set route-map-out6 { string } IPv6 Outbound route map filter. size[35] - datasource(s): router.route-map.name
set send-community { standard | extended | both | disable } IPv4 Send community attribute to neighbor.
    standard Standard.
    extended Extended.
    both Both.
    disable Disable
set send-community6 { standard | extended | both | disable } IPv6 Send community attribute to neighbor.
    standard Standard.
    extended Extended.
    both Both.
    disable Disable
set keep-alive-timer { integer } Keep alive timer interval (sec). range[0-65535]
set holdtime-timer { integer } Interval (sec) before peer considered dead. range[3-65535]
set connect-timer { integer } Interval (sec) for connect timer. range[0-65535]

```

```

    set unsuppress-map { string } IPv4 Route map to selectively unsuppress suppressed routes. size[35] - datasource(s): router.route-map.-
name
    set unsuppress-map6 { string } IPv6 Route map to selectively unsuppress suppressed routes. size[35] - datasource(s): router.route-
map.name
    set update-source { string } Interface to use as source IP/IPv6 address of TCP connections. size[15] - datasource(s): sys-
tem.interface.name
    set weight { integer } Neighbor weight. range[0-65535]
    set restart-time { integer } Graceful restart delay time (sec, 0 = global default). range[0-3600]
    set password { password_string } Password used in MD5 authentication. size[128]
    config conditional-advertise
        edit { advertise-routemap }
            # Conditional advertisement.
            set advertise-routemap { string } Name of advertising route map. size[35] - datasource(s): router.route-map.name
            set condition-routemap { string } Name of condition route map. size[35] - datasource(s): router.route-map.name
            set condition-type { exist | non-exist } Type of condition.
                exist True if condition route map is matched.
                non-exist True if condition route map is not matched.
        next
    next
config neighbor-group
    edit { name }
        # BGP neighbor group table.
        set name { string } Neighbor group name. size[45]
        set advertisement-interval { integer } Minimum interval (sec) between sending updates. range[1-600]
        set allowas-in-enable { enable | disable } Enable/disable IPv4 Enable to allow my AS in AS path.
        set allowas-in-enable6 { enable | disable } Enable/disable IPv6 Enable to allow my AS in AS path.
        set allowas-in { integer } IPv4 The maximum number of occurrence of my AS number allowed. range[1-10]
        set allowas-in6 { integer } IPv6 The maximum number of occurrence of my AS number allowed. range[1-10]
        set attribute-unchanged { as-path | med | next-hop } IPv4 List of attributes that should be unchanged.
            as-path AS path.
            med MED.
            next-hop Next hop.
        set attribute-unchanged6 { as-path | med | next-hop } IPv6 List of attributes that should be unchanged.
            as-path AS path.
            med MED.
            next-hop Next hop.
        set activate { enable | disable } Enable/disable address family IPv4 for this neighbor.
        set activate6 { enable | disable } Enable/disable address family IPv6 for this neighbor.
        set bfd { enable | disable } Enable/disable BFD for this neighbor.
        set capability-dynamic { enable | disable } Enable/disable advertise dynamic capability to this neighbor.
        set capability-orf { none | receive | send | both } Accept/Send IPv4 ORF lists to/from this neighbor.
            none None.
            receive Receive ORF lists.

```

```

        send      Send ORF list.
        both      Send and receive ORF lists.
set capability-orf6 { none | receive | send | both }  Accept/Send IPv6 ORF lists to/from this neighbor.
        none      None.
        receive   Receive ORF lists.
        send      Send ORF list.
        both      Send and receive ORF lists.
set capability-graceful-restart { enable | disable }  Enable/disable advertise IPv4 graceful restart capability to this neighbor.
set capability-graceful-restart6 { enable | disable }  Enable/disable advertise IPv6 graceful restart capability to this neighbor.
set capability-route-refresh { enable | disable }  Enable/disable advertise route refresh capability to this neighbor.
set capability-default-originate { enable | disable }  Enable/disable advertise default IPv4 route to this neighbor.
set capability-default-originate6 { enable | disable }  Enable/disable advertise default IPv6 route to this neighbor.
set dont-capability-negotiate { enable | disable }  Don't negotiate capabilities with this neighbor
set ebgp-enforce-multihop { enable | disable }  Enable/disable allow multi-hop EBGp neighbors.
set link-down-failover { enable | disable }  Enable/disable failover upon link down.
set stale-route { enable | disable }  Enable/disable stale route after neighbor down.
set next-hop-self { enable | disable }  Enable/disable IPv4 next-hop calculation for this neighbor.
set next-hop-self6 { enable | disable }  Enable/disable IPv6 next-hop calculation for this neighbor.
set override-capability { enable | disable }  Enable/disable override result of capability negotiation.
set passive { enable | disable }  Enable/disable sending of open messages to this neighbor.
set remove-private-as { enable | disable }  Enable/disable remove private AS number from IPv4 outbound updates.
set remove-private-as6 { enable | disable }  Enable/disable remove private AS number from IPv6 outbound updates.
set route-reflector-client { enable | disable }  Enable/disable IPv4 AS route reflector client.
set route-reflector-client6 { enable | disable }  Enable/disable IPv6 AS route reflector client.
set route-server-client { enable | disable }  Enable/disable IPv4 AS route server client.
set route-server-client6 { enable | disable }  Enable/disable IPv6 AS route server client.
set shutdown { enable | disable }  Enable/disable shutdown this neighbor.
set soft-reconfiguration { enable | disable }  Enable/disable allow IPv4 inbound soft reconfiguration.
set soft-reconfiguration6 { enable | disable }  Enable/disable allow IPv6 inbound soft reconfiguration.
set as-override { enable | disable }  Enable/disable replace peer AS with own AS for IPv4.
set as-override6 { enable | disable }  Enable/disable replace peer AS with own AS for IPv6.
set strict-capability-match { enable | disable }  Enable/disable strict capability matching.
set default-originate-routemap { string }  Route map to specify criteria to originate IPv4 default. size[35] - datasource(s): router-
.route-map.name
set default-originate-routemap6 { string }  Route map to specify criteria to originate IPv6 default. size[35] - datasource(s): router-
.route-map.name
set description { string }  Description. size[63]
set distribute-list-in { string }  Filter for IPv4 updates from this neighbor. size[35] - datasource(s): router.access-list.name
set distribute-list-in6 { string }  Filter for IPv6 updates from this neighbor. size[35] - datasource(s): router.access-list6.name
set distribute-list-out { string }  Filter for IPv4 updates to this neighbor. size[35] - datasource(s): router.access-list.name
set distribute-list-out6 { string }  Filter for IPv6 updates to this neighbor. size[35] - datasource(s): router.access-list6.name
set ebgp-multihop-ttl { integer }  EBGp multihop TTL for this peer. range[1-255]
set filter-list-in { string }  BGP filter for IPv4 inbound routes. size[35] - datasource(s): router.aspath-list.name

```

```

set filter-list-in6 { string } BGP filter for IPv6 inbound routes. size[35] - datasource(s): router.aspath-list.name
set filter-list-out { string } BGP filter for IPv4 outbound routes. size[35] - datasource(s): router.aspath-list.name
set filter-list-out6 { string } BGP filter for IPv6 outbound routes. size[35] - datasource(s): router.aspath-list.name
set interface { string } Interface size[15] - datasource(s): system.interface.name
set maximum-prefix { integer } Maximum number of IPv4 prefixes to accept from this peer. range[1-4294967295]
set maximum-prefix6 { integer } Maximum number of IPv6 prefixes to accept from this peer. range[1-4294967295]
set maximum-prefix-threshold { integer } Maximum IPv4 prefix threshold value (1 - 100 percent). range[1-100]
set maximum-prefix-threshold6 { integer } Maximum IPv6 prefix threshold value (1 - 100 percent). range[1-100]
set maximum-prefix-warning-only { enable | disable } Enable/disable IPv4 Only give warning message when limit is exceeded.
set maximum-prefix-warning-only6 { enable | disable } Enable/disable IPv6 Only give warning message when limit is exceeded.
set prefix-list-in { string } IPv4 Inbound filter for updates from this neighbor. size[35] - datasource(s): router.prefix-list.name
set prefix-list-in6 { string } IPv6 Inbound filter for updates from this neighbor. size[35] - datasource(s): router.prefix-list6.name
set prefix-list-out { string } IPv4 Outbound filter for updates to this neighbor. size[35] - datasource(s): router.prefix-list.name
set prefix-list-out6 { string } IPv6 Outbound filter for updates to this neighbor. size[35] - datasource(s): router.prefix-list6.name
set remote-as { integer } AS number of neighbor. range[1-4294967295]
set local-as { integer } Local AS number of neighbor. range[0-4294967295]
set local-as-no-prepend { enable | disable } Do not prepend local-as to incoming updates.
set local-as-replace-as { enable | disable } Replace real AS with local-as in outgoing updates.
set retain-stale-time { integer } Time to retain stale routes. range[0-65535]
set route-map-in { string } IPv4 Inbound route map filter. size[35] - datasource(s): router.route-map.name
set route-map-in6 { string } IPv6 Inbound route map filter. size[35] - datasource(s): router.route-map.name
set route-map-out { string } IPv4 Outbound route map filter. size[35] - datasource(s): router.route-map.name
set route-map-out6 { string } IPv6 Outbound route map filter. size[35] - datasource(s): router.route-map.name
set send-community { standard | extended | both | disable } IPv4 Send community attribute to neighbor.
    standard Standard.
    extended Extended.
    both Both.
    disable Disable
set send-community6 { standard | extended | both | disable } IPv6 Send community attribute to neighbor.
    standard Standard.
    extended Extended.
    both Both.
    disable Disable
set keep-alive-timer { integer } Keep alive timer interval (sec). range[0-65535]
set holdtime-timer { integer } Interval (sec) before peer considered dead. range[3-65535]
set connect-timer { integer } Interval (sec) for connect timer. range[0-65535]
set unsuppress-map { string } IPv4 Route map to selectively unsuppress suppressed routes. size[35] - datasource(s): router.route-map.-
name
set unsuppress-map6 { string } IPv6 Route map to selectively unsuppress suppressed routes. size[35] - datasource(s): router.route-
map.name
set update-source { string } Interface to use as source IP/IPv6 address of TCP connections. size[15] - datasource(s): sys-
tem.interface.name
set weight { integer } Neighbor weight. range[0-65535]

```

```
        set restart-time { integer } Graceful restart delay time (sec, 0 = global default). range[0-3600]
    next
config neighbor-range
    edit { id }
        # BGP neighbor range table.
        set id { integer } Neighbor range ID. range[0-4294967295]
        set prefix { ipv4 classnet } Neighbor range prefix.
        set max-neighbor-num { integer } Maximum number of neighbors. range[1-1000]
        set neighbor-group { string } Neighbor group name. size[63] - datasource(s): router.bgp.neighbor-group.name
    next
config network
    edit { id }
        # BGP network table.
        set id { integer } ID. range[0-4294967295]
        set prefix { ipv4 classnet } Network prefix.
        set backdoor { enable | disable } Enable/disable route as backdoor.
        set route-map { string } Route map to modify generated route. size[35] - datasource(s): router.route-map.name
    next
config network6
    edit { id }
        # BGP IPv6 network table.
        set id { integer } ID. range[0-4294967295]
        set prefix6 { ipv6 network } Network IPv6 prefix.
        set backdoor { enable | disable } Enable/disable route as backdoor.
        set route-map { string } Route map to modify generated route. size[35] - datasource(s): router.route-map.name
    next
config redistribute
    edit { name }
        # BGP IPv4 redistribute table.
        set name { string } Distribute list entry name. size[35]
        set status { enable | disable } Status
        set route-map { string } Route map name. size[35] - datasource(s): router.route-map.name
    next
config redistribute6
    edit { name }
        # BGP IPv6 redistribute table.
        set name { string } Distribute list entry name. size[35]
        set status { enable | disable } Status
        set route-map { string } Route map name. size[35] - datasource(s): router.route-map.name
    next
config admin-distance
    edit { id }
        # Administrative distance modifications.
```

```
set id { integer } ID. range[0-4294967295]
set neighbour-prefix { ipv4 classnet } Neighbor address prefix.
set route-list { string } Access list of routes to apply new distance to. size[35] - datasource(s): router.access-list.name
set distance { integer } Administrative distance to apply (1 - 255). range[1-255]
next
end
```

router community-list

Introduction.

```
config router community-list
  edit { name }
  # Configure community lists.
  set name { string } Community list name. size[35]
  set type { standard | expanded } Community list type (standard or expanded).
    standard Standard community list type.
    expanded Expanded community list type.
  config rule
    edit { id }
    # Community list rule.
    set id { integer } ID. range[0-4294967295]
    set action { deny | permit } Permit or deny route-based operations, based on the route's COMMUNITY attribute.
      deny Deny route-based operations.
      permit Permit or allow route-based operations.
    set regexp { string } Ordered list of COMMUNITY attributes as a regular expression. size[255]
    set match { string } Community specifications for matching a reserved community. size[255]
  next
next
end
```


router isis

Introduction.

```
config router isis
  set is-type { level-1-2 | level-1 | level-2-only } IS type.
    level-1-2    Level 1 and 2.
    level-1      Level 1 only.
    level-2-only Level 2 only.
  set auth-mode-l1 { password | md5 } Level 1 authentication mode.
    password Password.
    md5        MD5.
  set auth-mode-l2 { password | md5 } Level 2 authentication mode.
    password Password.
    md5        MD5.
  set auth-password-l1 { password_string } Authentication password for level 1 PDUs. size[128]
  set auth-password-l2 { password_string } Authentication password for level 2 PDUs. size[128]
  set auth-keychain-l1 { string } Authentication key-chain for level 1 PDUs. size[35] - datasource(s): router.key-chain.name
  set auth-keychain-l2 { string } Authentication key-chain for level 2 PDUs. size[35] - datasource(s): router.key-chain.name
  set auth-sendonly-l1 { enable | disable } Enable/disable level 1 authentication send-only.
  set auth-sendonly-l2 { enable | disable } Enable/disable level 2 authentication send-only.
  set ignore-lsp-errors { enable | disable } Enable/disable ignoring of LSP errors with bad checksums.
  set lsp-gen-interval-l1 { integer } Minimum interval for level 1 LSP regenerating. range[1-120]
  set lsp-gen-interval-l2 { integer } Minimum interval for level 2 LSP regenerating. range[1-120]
  set lsp-refresh-interval { integer } LSP refresh time in seconds. range[1-65535]
  set max-lsp-lifetime { integer } Maximum LSP lifetime in seconds. range[350-65535]
  set spf-interval-exp-l1 { string } Level 1 SPF calculation delay.
  set spf-interval-exp-l2 { string } Level 2 SPF calculation delay.
  set dynamic-hostname { enable | disable } Enable/disable dynamic hostname.
  set adjacency-check { enable | disable } Enable/disable adjacency check.
  set overload-bit { enable | disable } Enable/disable signal other routers not to use us in SPF.
  set overload-bit-suppress { external | interlevel } Suppress overload-bit for the specific prefixes.
    external External.
    interlevel Inter-level.
  set overload-bit-on-startup { integer } Overload-bit only temporarily after reboot. range[5-86400]
  set default-originate { enable | disable } Enable/disable control distribution of default information.
  set metric-style { option } Use old-style (ISO 10589) or new-style packet formats
    narrow Use old style of TLVs with narrow metric.
    narrow-transition Narrow and accept both styles of TLVs during transition.
```

```

    narrow-transition-l1  Narrow-transition level-1 only.
    narrow-transition-l2  Narrow-transition level-2 only.
    wide                  Use new style of TLVs to carry wider metric.
    wide-l1               Wide level-1 only.
    wide-l2               Wide level-2 only.
    wide-transition       Wide and accept both styles of TLVs during transition.
    wide-transition-l1    Wide-transition level-1 only.
    wide-transition-l2    Wide-transition level-2 only.
    transition            Send and accept both styles of TLVs during transition.
    transition-l1         Transition level-1 only.
    transition-l2         Transition level-2 only.
set redistribute-l1 { enable | disable }  Enable/disable redistribute level 1 routes into level 2.
set redistribute-l1-list { string }      Access-list for redistribute l1 to l2. size[35] - datasource(s): router.access-list.name
set redistribute-l2 { enable | disable }  Enable/disable redistribute level 2 routes into level 1.
set redistribute-l2-list { string }      Access-list for redistribute l2 to l1. size[35] - datasource(s): router.access-list.name
config isis-net
    edit { id }
        # IS-IS net configuration.
        set id { integer }  isis-net ID. range[0-4294967295]
        set net { string }  IS-IS net xx.xxxx. ... .xxxx.xx.
    next
config isis-interface
    edit { name }
        # IS-IS interface configuration.
        set name { string }  IS-IS interface name. size[15] - datasource(s): system.interface.name
        set status { enable | disable }  Enable/disable interface for IS-IS.
        set network-type { broadcast | point-to-point }  IS-IS interface's network type
            broadcast        Broadcast.
            point-to-point  Point-to-point.
        set circuit-type { level-1-2 | level-1 | level-2 }  IS-IS interface's circuit type
            level-1-2  Level 1 and 2.
            level-1    Level 1.
            level-2    Level 2.

        set csnp-interval-l1 { integer }  Level 1 CSNP interval. range[1-65535]
        set csnp-interval-l2 { integer }  Level 2 CSNP interval. range[1-65535]
        set hello-interval-l1 { integer }  Level 1 hello interval. range[0-65535]
        set hello-interval-l2 { integer }  Level 2 hello interval. range[0-65535]
        set hello-multiplier-l1 { integer }  Level 1 multiplier for Hello holding time. range[2-100]
        set hello-multiplier-l2 { integer }  Level 2 multiplier for Hello holding time. range[2-100]
        set hello-padding { enable | disable }  Enable/disable padding to IS-IS hello packets.
        set lsp-interval { integer }  LSP transmission interval (milliseconds). range[1-4294967295]
        set lsp-retransmit-interval { integer }  LSP retransmission interval (sec). range[1-65535]
        set metric-l1 { integer }  Level 1 metric for interface. range[1-63]

```

```

set metric-l2 { integer } Level 2 metric for interface. range[1-63]
set wide-metric-l1 { integer } Level 1 wide metric for interface. range[1-16777214]
set wide-metric-l2 { integer } Level 2 wide metric for interface. range[1-16777214]
set auth-password-l1 { password_string } Authentication password for level 1 PDUs. size[128]
set auth-password-l2 { password_string } Authentication password for level 2 PDUs. size[128]
set auth-keychain-l1 { string } Authentication key-chain for level 1 PDUs. size[35] - datasource(s): router.key-chain.name
set auth-keychain-l2 { string } Authentication key-chain for level 2 PDUs. size[35] - datasource(s): router.key-chain.name
set auth-send-only-l1 { enable | disable } Enable/disable authentication send-only for level 1 PDUs.
set auth-send-only-l2 { enable | disable } Enable/disable authentication send-only for level 2 PDUs.
set auth-mode-l1 { md5 | password } Level 1 authentication mode.
    md5 MD5.
    password Password.
set auth-mode-l2 { md5 | password } Level 2 authentication mode.
    md5 MD5.
    password Password.
set priority-l1 { integer } Level 1 priority. range[0-127]
set priority-l2 { integer } Level 2 priority. range[0-127]
set mesh-group { enable | disable } Enable/disable IS-IS mesh group.
set mesh-group-id { integer } Mesh group ID { 0-4294967295 }, 0: mesh-group blocked. range[0-4294967295]
next
config summary-address
edit { id }
# IS-IS summary addresses.
set id { integer } Summary address entry ID. range[0-4294967295]
set prefix { ipv4 classnet any } Prefix.
set level { level-1-2 | level-1 | level-2 } Level.
    level-1-2 Level 1 and 2.
    level-1 Level 1.
    level-2 Level 2.
next
config redistribute
edit { protocol }
# IS-IS redistribute protocols.
set protocol { string } Protocol name. size[35]
set status { enable | disable } Status.
set metric { integer } Metric. range[0-4261412864]
set metric-type { external | internal } Metric type.
    external External.
    internal Internal.
set level { level-1-2 | level-1 | level-2 } Level.
    level-1-2 Level 1 and 2.
    level-1 Level 1.
    level-2 Level 2.

```

```
        set routemap { string }  Route map name. size[35] - datasource(s): router.route-map.name
    next
end
```

router key-chain

Introduction.

```
config router key-chain
  edit { name }
  # Configure key-chain.
  set name { string }  Key-chain name. size[35]
  config key
    edit { id }
    # Configuration method to edit key settings.
    set id { integer }  Key ID (0 - 2147483647). range[0-2147483647]
    set accept-lifetime { string }  Lifetime of received authentication key (format: hh:mm:ss day month year).
    set send-lifetime { string }  Lifetime of sent authentication key (format: hh:mm:ss day month year).
    set key-string { string }  Password for the key (max. = 35 characters). size[35]
  next
next
end
```

router {multicast | multicast6}

Introduction.

```

config router multicast
    set route-threshold { integer }  Generate warnings when the number of multicast routes exceeds this number, must not be greater than route-
limit. range[1-2147483647]
    set route-limit { integer }  Maximum number of multicast routes. range[1-2147483647]
    set multicast-routing { enable | disable }  Enable/disable IP multicast routing.
    set message-interval { integer }  Period of time between sending periodic PIM join/prune messages in seconds (1 - 65535, default = 60).
range[1-65535]
    set join-prune-holdtime { integer }  Join/prune holdtime (1 - 65535, default = 210). range[1-65535]
    set accept-register-list { string }  Sources allowed to register packets with this Rendezvous Point (RP). size[35] - datasource(s): router-
.access-list.name
    set accept-source-list { string }  Sources allowed to send multicast traffic. size[35] - datasource(s): router.access-list.name
    set bsr-candidate { enable | disable }  Enable/disable allowing this router to become a bootstrap router (BSR).
    set bsr-interface { string }  Interface to advertise as candidate BSR. size[15] - datasource(s): system.interface.name
    set bsr-priority { integer }  BSR priority (0 - 255, default = 0). range[0-255]
    set bsr-hash { integer }  BSR hash length (0 - 32, default = 10). range[0-32]
    set bsr-allow-quick-refresh { enable | disable }  Enable/disable accept BSR quick refresh packets from neighbors.
    set cisco-register-checksum { enable | disable }  Checksum entire register packet(for old Cisco IOS compatibility).
    set cisco-register-checksum-group { string }  Cisco register checksum only these groups. size[35] - datasource(s): router.access-list.name
    set cisco-crp-prefix { enable | disable }  Enable/disable making candidate RP compatible with old Cisco IOS.
    set cisco-ignore-rp-set-priority { enable | disable }  Use only hash for RP selection (compatibility with old Cisco IOS).
    set register-rp-reachability { enable | disable }  Enable/disable check RP is reachable before registering packets.
    set register-source { disable | interface | ip-address }  Override source address in register packets.
        disable  Use source address of RPF interface.
        interface  Use primary IP of an interface.
        ip-address  Use a local IP address.
    set register-source-interface { string }  Override with primary interface address. size[15] - datasource(s): system.interface.name
    set register-source-ip { ipv4 address }  Override with local IP address.
    set register-suppression { integer }  Period of time to honor register-stop message (1 - 65535 sec, default = 60). range[1-65535]
    set null-register-retries { integer }  Maximum retries of null register (1 - 20, default = 1). range[1-20]
    set rp-register-keepalive { integer }  Timeout for RP receiving data on (S,G) tree (1 - 65535 sec, default = 185). range[1-65535]
    set spt-threshold { enable | disable }  Enable/disable switching to source specific trees.
    set spt-threshold-group { string }  Groups allowed to switch to source tree. size[35] - datasource(s): router.access-list.name
    set ssm { enable | disable }  Enable/disable source specific multicast.
    set ssm-range { string }  Groups allowed to source specific multicast. size[35] - datasource(s): router.access-list.name
    set register-rate-limit { integer }  Limit of packets/sec per source registered through this RP (0 - 65535, default = 0 which means

```

```

unlimited). range[0-65535]
  config rp-address
    edit { id }
    # Statically configure RP addresses.
    set id { integer } ID. range[0-4294967295]
    set ip-address { ipv4 address } RP router address.
    set group { string } Groups to use this RP. size[35] - datasource(s): router.access-list.name
  next
config interface
  edit { name }
  # PIM interfaces.
  set name { string } Interface name. size[15] - datasource(s): system.interface.name
  set ttl-threshold { integer } Minimum TTL of multicast packets that will be forwarded (applied only to new multicast routes) (1 - 255,
default = 1). range[1-255]
  set pim-mode { sparse-mode | dense-mode } PIM operation mode.
    sparse-mode sparse-mode
    dense-mode dense-mode
  set passive { enable | disable } Enable/disable listening to IGMP but not participating in PIM.
  set bfd { enable | disable } Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).
  set neighbour-filter { string } Routers acknowledged as neighbor routers. size[35] - datasource(s): router.access-list.name
  set hello-interval { integer } Interval between sending PIM hello messages (0 - 65535 sec, default = 30). range[1-65535]
  set hello-holdtime { integer } Time before old neighbor information expires (0 - 65535 sec, default = 105). range[1-65535]
  set cisco-exclude-genid { enable | disable } Exclude GenID from hello packets (compatibility with old Cisco IOS).
  set dr-priority { integer } DR election priority. range[1-4294967295]
  set propagation-delay { integer } Delay flooding packets on this interface (100 - 5000 msec, default = 500). range[100-5000]
  set state-refresh-interval { integer } Interval between sending state-refresh packets (1 - 100 sec, default = 60). range[1-100]
  set rp-candidate { enable | disable } Enable/disable compete to become RP in elections.
  set rp-candidate-group { string } Multicast groups managed by this RP. size[35] - datasource(s): router.access-list.name
  set rp-candidate-priority { integer } Router's priority as RP. range[0-255]
  set rp-candidate-interval { integer } RP candidate advertisement interval (1 - 16383 sec, default = 60). range[1-16383]
  set multicast-flow { string } Acceptable source for multicast group. size[35] - datasource(s): router.multicast-flow.name
  set static-group { string } Statically set multicast groups to forward out. size[35] - datasource(s): router.multicast-flow.name
  config join-group
    edit { address }
    # Join multicast groups.
    set address { ipv4 address any } Multicast group IP address.
  next
  set access-group { string } Groups IGMP hosts are allowed to join. size[35] - datasource(s): router.access-list.name
  set version { 3 | 2 | 1 } Maximum version of IGMP to support.
    3 Version 3 and lower.
    2 Version 2 and lower.
    1 Version 1.
  set immediate-leave-group { string } Groups to drop membership for immediately after receiving IGMPv2 leave. size[35] - datasource

```

```
(s): router.access-list.name
    set last-member-query-interval { integer } Timeout between IGMPv2 leave and removing group (1 - 65535 msec, default = 1000). range
[1-65535]
    set last-member-query-count { integer } Number of group specific queries before removing group (2 - 7, default = 2). range[2-7]
    set query-max-response-time { integer } Maximum time to wait for a IGMP query response (1 - 25 sec, default = 10). range[1-25]
    set query-interval { integer } Interval between queries to IGMP hosts (1 - 65535 sec, default = 125). range[1-65535]
    set query-timeout { integer } Timeout between queries before becoming querier for network (60 - 900, default = 255). range[60-900]
    set router-alert-check { enable | disable } Enable/disable require IGMP packets contain router alert option.
    next
end

config router multicast6
    set multicast-routing { enable | disable } Enable/disable IPv6 multicast routing.
    set multicast-pmtu { enable | disable } Enable/disable PMTU for IPv6 multicast.
    config interface
        edit { name }
            # Protocol Independent Multicast (PIM) interfaces.
            set name { string } Interface name. size[15] - datasource(s): system.interface.name
            set hello-interval { integer } Interval between sending PIM hello messages (1 - 65535 sec, default = 30).. range[1-65535]
            set hello-holdtime { integer } Time before old neighbour information expires (1 - 65535 sec, default = 105). range[1-65535]
        next
        set register-rate-limit { integer } Limit of packets/sec per source registered through this RP (0 means unlimited). range[0-65535]
        config rp-address
            edit { id }
                # Statically configured RP addresses.
                set id { integer } ID of the entry. range[0-4294967295]
                set ipv6-address { ipv6 address } RP router IPv6 address.
            next
        end
    end
```


router multicast-flow

Introduction.

```
config router multicast-flow
  edit { name }
  # Configure multicast-flow.
  set name { string } Name. size[35]
  set comments { string } Comment. size[127]
  config flows
    edit { id }
    # Multicast-flow entries.
    set id { integer } Flow ID. range[0-4294967295]
    set group-addr { ipv4 address any } Multicast group IP address.
    set source-addr { ipv4 address any } Multicast source IP address.
  next
next
end
```

router {ospf | ospf6}

Introduction.

```

config router ospf
  set abr-type { cisco | ibm | shortcut | standard } Area border router type.
    cisco      Cisco.
    ibm        IBM.
    shortcut   Shortcut.
    standard   Standard.
  set auto-cost-ref-bandwidth { integer } Reference bandwidth in terms of megabits per second. range[1-1000000]
  set distance-external { integer } Administrative external distance. range[1-255]
  set distance-inter-area { integer } Administrative inter-area distance. range[1-255]
  set distance-intra-area { integer } Administrative intra-area distance. range[1-255]
  set database-overflow { enable | disable } Enable/disable database overflow.
  set database-overflow-max-lsas { integer } Database overflow maximum LSAs. range[0-4294967295]
  set database-overflow-time-to-recover { integer } Database overflow time to recover (sec). range[0-65535]
  set default-information-originate { enable | always | disable } Enable/disable generation of default route.
  set default-information-metric { integer } Default information metric. range[1-16777214]
  set default-information-metric-type { 1 | 2 } Default information metric type.
    1 Type 1.
    2 Type 2.
  set default-information-route-map { string } Default information route map. size[35] - datasource(s): router.route-map.name
  set default-metric { integer } Default metric of redistribute routes. range[1-16777214]
  set distance { integer } Distance of the route. range[1-255]
  set rfc1583-compatible { enable | disable } Enable/disable RFC1583 compatibility.
  set router-id { ipv4 address any } Router ID.
  set spf-timers { string } SPF calculation frequency.
  set bfd { enable | disable } Bidirectional Forwarding Detection (BFD).
  set log-neighbour-changes { enable | disable } Enable logging of OSPF neighbour's changes
  set distribute-list-in { string } Filter incoming routes. size[35] - datasource(s): router.access-list.name,router.prefix-list.name
  set distribute-route-map-in { string } Filter incoming external routes by route-map. size[35] - datasource(s): router.route-map.name
  set restart-mode { none | lls | graceful-restart } OSPF restart mode (graceful or LLS).
    none          Hitless restart disabled.
    lls           LLS mode.
    graceful-restart Graceful Restart Mode.
  set restart-period { integer } Graceful restart period. range[1-3600]
config area
  edit { id }

```

```

# OSPF area configuration.
set id { ipv4 address any } Area entry IP address.
set shortcut { disable | enable | default } Enable/disable shortcut option.
set authentication { none | text | md5 } Authentication type.
    none None.
    text Text.
    md5 MD5.
set default-cost { integer } Summary default cost of stub or NSSA area. range[0-4294967295]
set nssa-translator-role { candidate | never | always } NSSA translator role type.
    candidate Candidate.
    never Never.
    always Always.
set stub-type { no-summary | summary } Stub summary setting.
    no-summary No summary.
    summary Summary.
set type { regular | nssa | stub } Area type setting.
    regular Regular.
    nssa NSSA.
    stub Stub.
set nssa-default-information-originate { enable | always | disable } Redistribute, advertise, or do not originate Type-7 default route
into NSSA area.
set nssa-default-information-originate-metric { integer } OSPF default metric. range[0-16777214]
set nssa-default-information-originate-metric-type { 1 | 2 } OSPF metric type for default routes.
    1 Type 1.
    2 Type 2.
set nssa-redistribution { enable | disable } Enable/disable redistribute into NSSA area.
config range
edit { id }
# OSPF area range configuration.
set id { integer } Range entry ID. range[0-4294967295]
set prefix { ipv4 classnet any } Prefix.
set advertise { disable | enable } Enable/disable advertise status.
set substitute { ipv4 classnet any } Substitute prefix.
set substitute-status { enable | disable } Enable/disable substitute status.
next
config virtual-link
edit { name }
# OSPF virtual link configuration.
set name { string } Virtual link entry name. size[35]
set authentication { none | text | md5 } Authentication type.
    none None.
    text Text.
    md5 MD5.

```

```

    set authentication-key { password_string } Authentication key. size[8]
    set md5-key { string } MD5 key.
    set dead-interval { integer } Dead interval. range[1-65535]
    set hello-interval { integer } Hello interval. range[1-65535]
    set retransmit-interval { integer } Retransmit interval. range[1-65535]
    set transmit-delay { integer } Transmit delay. range[1-65535]
    set peer { ipv4 address any } Peer IP.
  next
config filter-list
  edit { id }
  # OSPF area filter-list configuration.
  set id { integer } Filter list entry ID. range[0-4294967295]
  set list { string } Access-list or prefix-list name. size[35] - datasource(s): router.access-list.name,router.prefix-list.name
  set direction { in | out } Direction.
    in In.
    out Out.
  next
next
config ospf-interface
  edit { name }
  # OSPF interface configuration.
  set name { string } Interface entry name. size[35]
  set interface { string } Configuration interface name. size[15] - datasource(s): system.interface.name
  set ip { ipv4 address } IP address.
  set authentication { none | text | md5 } Authentication type.
    none None.
    text Text.
    md5 MD5.
  set authentication-key { password_string } Authentication key. size[8]
  set md5-key { string } MD5 key.
  set prefix-length { integer } Prefix length. range[0-32]
  set retransmit-interval { integer } Retransmit interval. range[1-65535]
  set transmit-delay { integer } Transmit delay. range[1-65535]
  set cost { integer } Cost of the interface, value range from 0 to 65535, 0 means auto-cost. range[0-65535]
  set priority { integer } Priority. range[0-255]
  set dead-interval { integer } Dead interval. range[0-65535]
  set hello-interval { integer } Hello interval. range[0-65535]
  set hello-multiplier { integer } Number of hello packets within dead interval. range[3-10]
  set database-filter-out { enable | disable } Enable/disable control of flooding out LSAs.
  set mtu { integer } MTU for database description packets. range[576-65535]
  set mtu-ignore { enable | disable } Enable/disable ignore MTU.
  set network-type { option } Network type.
    broadcast Broadcast.

```

```

        non-broadcast                Non-broadcast.
        point-to-point               Point-to-point.
        point-to-multipoint          Point-to-multipoint.
        point-to-multipoint-non-broadcast Point-to-multipoint and non-broadcast.
    set bfd { global | enable | disable } Bidirectional Forwarding Detection (BFD).
    set status { disable | enable } Enable/disable status.
    set resync-timeout { integer } Graceful restart neighbor resynchronization timeout. range[1-3600]
next
config network
edit { id }
# OSPF network configuration.
    set id { integer } Network entry ID. range[0-4294967295]
    set prefix { ipv4 classnet } Prefix.
    set area { ipv4 address any } Attach the network to area.
next
config neighbor
edit { id }
# OSPF neighbor configuration are used when OSPF runs on non-broadcast media
    set id { integer } Neighbor entry ID. range[0-4294967295]
    set ip { ipv4 address } Interface IP address of the neighbor.
    set poll-interval { integer } Poll interval time in seconds. range[1-65535]
    set cost { integer } Cost of the interface, value range from 0 to 65535, 0 means auto-cost. range[0-65535]
    set priority { integer } Priority. range[0-255]
next
config passive-interface
edit { name }
# Passive interface configuration.
    set name { string } Passive interface name. size[64] - datasource(s): system.interface.name
next
config summary-address
edit { id }
# IP address summary configuration.
    set id { integer } Summary address entry ID. range[0-4294967295]
    set prefix { ipv4 classnet } Prefix.
    set tag { integer } Tag value. range[0-4294967295]
    set advertise { disable | enable } Enable/disable advertise status.
next
config distribute-list
edit { id }
# Distribute list configuration.
    set id { integer } Distribute list entry ID. range[0-4294967295]
    set access-list { string } Access list name. size[35] - datasource(s): router.access-list.name
    set protocol { connected | static | rip } Protocol type.

```

```

        connected Connected type.
        static      Static type.
        rip         RIP type.
    next
config redistribute
edit { name }
# Redistribute configuration.
set name { string }  Redistribute name. size[35]
set status { enable | disable }  status
set metric { integer }  Redistribute metric setting. range[1-16777214]
set routemap { string }  Route map name. size[35] - datasource(s): router.route-map.name
set metric-type { 1 | 2 }  Metric type.
    1 Type 1.
    2 Type 2.
set tag { integer }  Tag value. range[0-4294967295]
next
end

config router ospf6
set abr-type { cisco | ibm | standard }  Area border router type.
    cisco Cisco.
    ibm IBM.
    standard Standard.
set auto-cost-ref-bandwidth { integer }  Reference bandwidth in terms of megabits per second. range[1-1000000]
set default-information-originate { enable | always | disable }  Enable/disable generation of default route.
set log-neighbour-changes { enable | disable }  Enable logging of OSPFv3 neighbour's changes
set default-information-metric { integer }  Default information metric. range[1-16777214]
set default-information-metric-type { 1 | 2 }  Default information metric type.
    1 Type 1.
    2 Type 2.
set default-information-route-map { string }  Default information route map. size[35] - datasource(s): router.route-map.name
set default-metric { integer }  Default metric of redistribute routes. range[1-16777214]
set router-id { ipv4 address any }  A.B.C.D, in IPv4 address format.
set spf-timers { string }  SPF calculation frequency.
config area
edit { id }
# OSPF6 area configuration.
set id { ipv4 address any }  Area entry IP address.
set default-cost { integer }  Summary default cost of stub or NSSA area. range[0-16777215]
set nssa-translator-role { candidate | never | always }  NSSA translator role type.
    candidate Candidate.
    never Never.

```

```

        always      Always.
set stub-type { no-summary | summary }  Stub summary setting.
        no-summary  No summary.
        summary     Summary.
set type { regular | nssa | stub }  Area type setting.
        regular    Regular.
        nssa       NSSA.
        stub       Stub.

set nssa-default-information-originate { enable | disable }  Enable/disable originate type 7 default into NSSA area.
set nssa-default-information-originate-metric { integer }  OSPFv3 default metric. range[0-16777214]
set nssa-default-information-originate-metric-type { 1 | 2 }  OSPFv3 metric type for default routes.
        1  Type 1.
        2  Type 2.
set nssa-redistribution { enable | disable }  Enable/disable redistribute into NSSA area.
config range
    edit { id }
        # OSPF6 area range configuration.
        set id { integer }  Range entry ID. range[0-4294967295]
        set prefix6 { ipv6 network }  IPv6 prefix.
        set advertise { disable | enable }  Enable/disable advertise status.
    next
config virtual-link
    edit { name }
        # OSPF6 virtual link configuration.
        set name { string }  Virtual link entry name. size[35]
        set dead-interval { integer }  Dead interval. range[1-65535]
        set hello-interval { integer }  Hello interval. range[1-65535]
        set retransmit-interval { integer }  Retransmit interval. range[1-65535]
        set transmit-delay { integer }  Transmit delay. range[1-65535]
        set peer { ipv4 address any }  A.B.C.D, peer router ID.
    next
next
config ospf6-interface
    edit { name }
        # OSPF6 interface configuration.
        set name { string }  Interface entry name. size[35]
        set area-id { ipv4 address any }  A.B.C.D, in IPv4 address format.
        set interface { string }  Configuration interface name. size[15] - datasource(s): system.interface.name
        set retransmit-interval { integer }  Retransmit interval. range[1-65535]
        set transmit-delay { integer }  Transmit delay. range[1-65535]
        set cost { integer }  Cost of the interface, value range from 0 to 65535, 0 means auto-cost. range[0-65535]
        set priority { integer }  priority range[0-255]
        set dead-interval { integer }  Dead interval. range[1-65535]

```

```
set hello-interval { integer } Hello interval. range[1-65535]
set status { disable | enable } Enable/disable OSPF6 routing on this interface.
set network-type { option } Network type.
    broadcast broadcast
    non-broadcast non-broadcast
    point-to-point point-to-point
    point-to-multipoint point-to-multipoint
    point-to-multipoint-non-broadcast point-to-multipoint and non-broadcast.
config neighbor
    edit { ip6 }
        # OSPFv3 neighbors are used when OSPFv3 runs on non-broadcast media
        set ip6 { ipv6 address } IPv6 link local address of the neighbor.
        set poll-interval { integer } Poll interval time in seconds. range[1-65535]
        set cost { integer } Cost of the interface, value range from 0 to 65535, 0 means auto-cost. range[0-65535]
        set priority { integer } priority range[0-255]
    next
next
config passive-interface
    edit { name }
        # Passive interface configuration.
        set name { string } Passive interface name. size[64] - datasource(s): system.interface.name
    next
config redistribute
    edit { name }
        # Redistribute configuration.
        set name { string } Redistribute name. size[35]
        set status { enable | disable } status
        set metric { integer } Redistribute metric setting. range[1-16777214]
        set routemap { string } Route map name. size[35] - datasource(s): router.route-map.name
        set metric-type { 1 | 2 } Metric type.
            1 Type 1.
            2 Type 2.
    next
config summary-address
    edit { id }
        # IPv6 address summary configuration.
        set id { integer } Summary address entry ID. range[0-4294967295]
        set prefix6 { ipv6 network } IPv6 prefix.
        set advertise { disable | enable } Enable/disable advertise status.
        set tag { integer } Tag value. range[0-4294967295]
    next
end
```


router {policy | policy6}

Introduction.

```
config router policy
  edit { seq-num }
  # Configure IPv4 routing policies.
  set seq-num { integer } Sequence number. range[0-4294967295]
  config input-device
    edit { name }
    # Incoming interface name.
    set name { string } Interface name. size[64] - datasource(s): system.interface.name
  next
  config src
    edit { subnet }
    # Source IP and mask (x.x.x.x/x).
    set subnet { string } IP and mask. size[64]
  next
  config srcaddr
    edit { name }
    # Source address name.
    set name { string } Address/group name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  set src-negate { enable | disable } Enable/disable negating source address match.
  config dst
    edit { subnet }
    # Destination IP and mask (x.x.x.x/x).
    set subnet { string } IP and mask. size[64]
  next
  config dstaddr
    edit { name }
    # Destination address name.
    set name { string } Address/group name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  set dst-negate { enable | disable } Enable/disable negating destination address match.
  set action { deny | permit } Action of the policy route.
  deny Do not search policy route table.
  permit Use this policy route for forwarding.
  set protocol { integer } Protocol number (0 - 255). range[0-255]
```

```
set start-port { integer } Start destination port number (0 - 65535). range[0-65535]
set end-port { integer } End destination port number (0 - 65535). range[0-65535]
set start-source-port { integer } Start source port number (0 - 65535). range[0-65535]
set end-source-port { integer } End source port number (0 - 65535). range[0-65535]
set gateway { ipv4 address } IP address of the gateway.
set output-device { string } Outgoing interface name. size[35] - datasource(s): system.interface.name
set tos { string } Type of service bit pattern.
set tos-mask { string } Type of service evaluated bits.
set status { enable | disable } Enable/disable this policy route.
set comments { string } Optional comments. size[255]
next
end

config router policy6
edit { seq-num }
# Configure IPv6 routing policies.
set seq-num { integer } Sequence number. range[0-4294967295]
set input-device { string } Incoming interface name. size[35] - datasource(s): system.interface.name
set src { ipv6 network } Source IPv6 prefix.
set dst { ipv6 network } Destination IPv6 prefix.
set protocol { integer } Protocol number (0 - 255). range[0-255]
set start-port { integer } Start destination port number (1 - 65535). range[1-65535]
set end-port { integer } End destination port number (1 - 65535). range[1-65535]
set gateway { ipv6 address } IPv6 address of the gateway.
set output-device { string } Outgoing interface name. size[35] - datasource(s): system.interface.name
set tos { string } Type of service bit pattern.
set tos-mask { string } Type of service evaluated bits.
set status { enable | disable } Enable/disable this policy route.
set comments { string } Optional comments. size[255]
next
end
```

router {prefix-list | prefix-list6}

Introduction.

```
config router prefix-list
  edit { name }
  # Configure IPv4 prefix lists.
  set name { string } Name. size[35]
  set comments { string } Comment. size[127]
  config rule
  edit { id }
  # IPv4 prefix list rule.
  set id { integer } Rule ID. range[0-4294967295]
  set action { permit | deny } Permit or deny this IP address and netmask prefix.
    permit Allow or permit packets that match this rule.
    deny Deny packets that match this rule.
  set prefix { string } IPv4 prefix to define regular filter criteria, such as "any" or subnets.
  set ge { integer } Minimum prefix length to be matched (0 - 32). range[0-32]
  set le { integer } Maximum prefix length to be matched (0 - 32). range[0-32]
  set flags { integer } Flags. range[0-4294967295]
  next
next
end

config router prefix-list6
  edit { name }
  # Configure IPv6 prefix lists.
  set name { string } Name. size[35]
  set comments { string } Comment. size[127]
  config rule
  edit { id }
  # IPv6 prefix list rule.
  set id { integer } Rule ID. range[0-4294967295]
  set action { permit | deny } Permit or deny packets that match this rule.
    permit Allow or permit packets that match this rule.
    deny Deny packets that match this rule.
  set prefix6 { string } IPv6 prefix to define regular filter criteria, such as "any" or subnets.
```

```
        set ge { integer }  Minimum prefix length to be matched (0 - 128). range[0-128]
        set le { integer }  Maximum prefix length to be matched (0 - 128). range[0-128]
        set flags { integer }  Flags. range[0-4294967295]
    next
end
```

router rip

Introduction.

```
config router rip
  set default-information-originate { enable | disable } Enable/disable generation of default route.
  set default-metric { integer } Default metric. range[1-16]
  set max-out-metric { integer } Maximum metric allowed to output(0 means 'not set'). range[0-15]
  set recv-buffer-size { integer } Receiving buffer size. range[8129-2147483647]
  config distance
    edit { id }
      # distance
      set id { integer } Distance ID. range[0-4294967295]
      set prefix { ipv4 classnet any } Distance prefix.
      set distance { integer } Distance (1 - 255). range[1-255]
      set access-list { string } Access list for route destination. size[35] - datasource(s): router.access-list.name
    next
  config distribute-list
    edit { id }
      # Distribute list.
      set id { integer } Distribute list ID. range[0-4294967295]
      set status { enable | disable } status
      set direction { in | out } Distribute list direction.
        in Filter incoming packets.
        out Filter outgoing packets.
      set listname { string } Distribute access/prefix list name. size[35] - datasource(s): router.access-list.name,router.prefix-list.name
      set interface { string } Distribute list interface name. size[15] - datasource(s): system.interface.name
    next
  config neighbor
    edit { id }
      # neighbor
      set id { integer } Neighbor entry ID. range[0-4294967295]
      set ip { ipv4 address } IP address.
    next
  config network
    edit { id }
      # network
      set id { integer } Network entry ID. range[0-4294967295]
      set prefix { ipv4 classnet } Network prefix.
```

```
next
config offset-list
edit { id }
# Offset list.
set id { integer } Offset-list ID. range[0-4294967295]
set status { enable | disable } status
set direction { in | out } Offset list direction.
    in Filter incoming packets.
    out Filter outgoing packets.
set access-list { string } Access list name. size[35] - datasource(s): router.access-list.name
set offset { integer } offset range[1-16]
set interface { string } Interface name. size[15] - datasource(s): system.interface.name
next
config passive-interface
edit { name }
# Passive interface configuration.
set name { string } Passive interface name. size[64] - datasource(s): system.interface.name
next
config redistribute
edit { name }
# Redistribute configuration.
set name { string } Redistribute name. size[35]
set status { enable | disable } status
set metric { integer } Redistribute metric setting. range[0-16777214]
set routemap { string } Route map name. size[35] - datasource(s): router.route-map.name
next
set update-timer { integer } Update timer in seconds. range[5-2147483647]
set timeout-timer { integer } Timeout timer in seconds. range[5-2147483647]
set garbage-timer { integer } Garbage timer in seconds. range[5-2147483647]
set version { 1 | 2 } RIP version.
    1 Version 1.
    2 Version 2.
config interface
edit { name }
# RIP interface configuration.
set name { string } Interface name. size[35] - datasource(s): system.interface.name
set auth-keychain { string } Authentication key-chain name. size[35] - datasource(s): router.key-chain.name
set auth-mode { none | text | md5 } Authentication mode.
    none None.
    text Text.
    md5 MD5.
set auth-string { password_string } Authentication string/password. size[16]
set receive-version { 1 | 2 } Receive version.
```

```
    1 Version 1.
    2 Version 2.
set send-version { 1 | 2 }  Send version.
    1 Version 1.
    2 Version 2.
set send-version2-broadcast { disable | enable }  Enable/disable broadcast version 1 compatible packets.
set split-horizon-status { enable | disable }  Enable/disable split horizon.
set split-horizon { poisoned | regular }  Enable/disable split horizon.
    poisoned Poisoned.
    regular Regular.
set flags { integer }  flags range[0-255]
next
end
```

router ripng

Introduction.

```
config router ripng
  set default-information-originate { enable | disable }  Enable/disable generation of default route.
  set default-metric { integer }  Default metric. range[1-16]
  set max-out-metric { integer }  Maximum metric allowed to output(0 means 'not set'). range[0-15]
  config distance
    edit { id }
    # distance
    set id { integer }  Distance ID. range[0-4294967295]
    set distance { integer }  Distance (1 - 255). range[1-255]
    set prefix6 { ipv6 prefix }  Distance prefix6.
    set access-list6 { string }  Access list for route destination. size[35] - datasource(s): router.access-list6.name
  next
  config distribute-list
    edit { id }
    # Distribute list.
    set id { integer }  Distribute list ID. range[0-4294967295]
    set status { enable | disable }  status
    set direction { in | out }  Distribute list direction.
      in  Filter incoming packets.
      out Filter outgoing packets.
    set listname { string }  Distribute access/prefix list name. size[35] - datasource(s): router.access-list6.name,router.prefix-list6.name
    set interface { string }  Distribute list interface name. size[15] - datasource(s): system.interface.name
  next
  config neighbor
    edit { id }
    # neighbor
    set id { integer }  Neighbor entry ID. range[0-4294967295]
    set ip6 { ipv6 address }  IPv6 link-local address.
    set interface { string }  Interface name. size[15] - datasource(s): system.interface.name
  next
  config network
    edit { id }
    # Network.
    set id { integer }  Network entry ID. range[0-4294967295]
    set prefix { ipv6 prefix }  Network IPv6 link-local prefix.
```



```
next
config aggregate-address
edit { id }
# Aggregate address.
set id { integer } Aggregate address entry ID. range[0-4294967295]
set prefix6 { ipv6 prefix } Aggregate address prefix.
next
config offset-list
edit { id }
# Offset list.
set id { integer } Offset-list ID. range[0-4294967295]
set status { enable | disable } status
set direction { in | out } Offset list direction.
in Filter incoming packets.
out Filter outgoing packets.
set access-list6 { string } IPv6 access list name. size[35] - datasource(s): router.access-list6.name
set offset { integer } offset range[1-16]
set interface { string } Interface name. size[15] - datasource(s): system.interface.name
next
config passive-interface
edit { name }
# Passive interface configuration.
set name { string } Passive interface name. size[64] - datasource(s): system.interface.name
next
config redistribute
edit { name }
# Redistribute configuration.
set name { string } Redistribute name. size[35]
set status { enable | disable } status
set metric { integer } Redistribute metric setting. range[0-16777214]
set routemap { string } Route map name. size[35] - datasource(s): router.route-map.name
next
set update-timer { integer } Update timer. range[5-2147483647]
set timeout-timer { integer } Timeout timer. range[5-2147483647]
set garbage-timer { integer } Garbage timer. range[5-2147483647]
config interface
edit { name }
# RIPng interface configuration.
set name { string } Interface name. size[35] - datasource(s): system.interface.name
set split-horizon-status { enable | disable } Enable/disable split horizon.
set split-horizon { poisoned | regular } Enable/disable split horizon.
poisoned Poisoned.
regular Regular.
```

```
        set flags { integer } Flags.range[0-255]
    next
end
```

router route-map

Introduction.

```

config router route-map
  edit { name }
  # Configure route maps.
  set name { string } Name. size[35]
  set comments { string } Optional comments. size[127]
  config rule
  edit { id }
  # Rule.
  set id { integer } Rule ID. range[0-4294967295]
  set action { permit | deny } Action.
    permit Permit.
    deny Deny.
  set match-as-path { string } Match BGP AS path list. size[35] - datasource(s): router.aspath-list.name
  set match-community { string } Match BGP community list. size[35] - datasource(s): router.community-list.name
  set match-community-exact { enable | disable } Enable/disable exact matching of communities.
  set match-origin { none | egp | igp | incomplete } Match BGP origin code.
    none None.
    egp Remote EGP.
    igp Local IGP.
    incomplete Unknown heritage.
  set match-interface { string } Match interface configuration. size[15] - datasource(s): system.interface.name
  set match-ip-address { string } Match IP address permitted by access-list or prefix-list. size[35] - datasource(s): router.access-
list.name,router.prefix-list.name
  set match-ip6-address { string } Match IPv6 address permitted by access-list6 or prefix-list6. size[35] - datasource(s): router-
.access-list6.name,router.prefix-list6.name
  set match-ip-nexthop { string } Match next hop IP address passed by access-list or prefix-list. size[35] - datasource(s): router-
.access-list.name,router.prefix-list.name
  set match-ip6-nexthop { string } Match next hop IPv6 address passed by access-list6 or prefix-list6. size[35] - datasource(s):
router.access-list6.name,router.prefix-list6.name
  set match-metric { integer } Match metric for redistribute routes. range[0-4294967295]
  set match-route-type { 1 | 2 | none } Match route type.
    1 External type 1.
    2 External type 2.
    none No type specified.
  set match-tag { integer } Match tag. range[0-4294967295]

```

```

set set-aggregator-as { integer }   BGP aggregator AS. range[1-4294967295]
set set-aggregator-ip { ipv4 address any }   BGP aggregator IP.
set set-aspath-action { prepend | replace }   Specify preferred action of set-aspath.
    prepend Prepend.
    replace Replace.
config set-aspath
    edit { as }
    # Prepend BGP AS path attribute.
    set as { string }   AS number (0 - 42949672). NOTE: Use quotes for repeating numbers, e.g.: "1 1 2"
size[64]
    next
set set-atomic-aggregate { enable | disable }   Enable/disable BGP atomic aggregate attribute.
set set-community-delete { string }   Delete communities matching community list. size[35] - datasource(s): router.community-list.-
name
config set-community
    edit { community }
    # BGP community attribute.
    set community { string }   Attribute: AA|AA:NN|internet|local-AS|no-advertise|no-export. size[64]
    next
set set-community-additive { enable | disable }   Enable/disable adding set-community to existing community.
set set-dampening-reachability-half-life { integer }   Reachability half-life time for the penalty (1 - 45 min). range[1-45]
set set-dampening-reuse { integer }   Value to start reusing a route (1 - 20000). range[1-20000]
set set-dampening-suppress { integer }   Value to start suppressing a route (1 - 20000). range[1-20000]
set set-dampening-max-suppress { integer }   Maximum duration to suppress a route (1 - 255 min). range[1-255]
set set-dampening-unreachability-half-life { integer }   Unreachability Half-life time for the penalty (1 - 45 min) range[1-45]
config set-extcommunity-rt
    edit { community }
    # Route Target extended community.
    set community { string }   AA:NN. size[64]
    next
config set-extcommunity-soo
    edit { community }
    # Site-of-Origin extended community.
    set community { string }   AA:NN size[64]
    next
set set-ip-nexthop { ipv4 address }   IP address of next hop.
set set-ip6-nexthop { ipv6 address }   IPv6 global address of next hop.
set set-ip6-nexthop-local { ipv6 address }   IPv6 local address of next hop.
set set-local-preference { integer }   BGP local preference path attribute. range[0-4294967295]
set set-metric { integer }   Metric value. range[0-4294967295]
set set-metric-type { 1 | 2 | none }   Metric type.
    1   External type 1.
    2   External type 2.

```

```
        none No type specified.
set set-originator-id { ipv4 address any } BGP originator ID attribute.
set set-origin { none | egp | igp | incomplete } BGP origin code.
    none      None.
    egp       Remote EGP.
    igp       Local IGP.
    incomplete Unknown heritage.
set set-tag { integer } Tag value. range[0-4294967295]
set set-weight { integer } BGP weight for routing table. range[0-4294967295]
set set-flags { integer } BGP flags value (0 - 65535) range[0-65535]
set match-flags { integer } BGP flag value to match (0 - 65535) range[0-65535]
next
end
```

router setting

Introduction.

```
config router setting
  set show-filter { string } Prefix-list as filter for showing routes. size[35] - datasource(s): router.prefix-list.name
  set hostname { string } Hostname for this virtual domain router. size[14]
end
```

router {static | static6}

Introduction.

```

config router static
  edit { seq-num }
  # Configure IPv4 static routing tables.
  set seq-num { integer } Sequence number. range[0-4294967295]
  set status { enable | disable } Enable/disable this static route.
  set dst { ipv4 classnet } Destination IP and mask for this route.
  set gateway { ipv4 address } Gateway IP for this route.
  set distance { integer } Administrative distance (1 - 255). range[1-255]
  set weight { integer } Administrative weight (0 - 255). range[0-255]
  set priority { integer } Administrative priority (0 - 4294967295). range[0-4294967295]
  set device { string } Gateway out interface or tunnel. size[35] - datasource(s): system.interface.name
  set comment { string } Optional comments. size[255]
  set blackhole { enable | disable } Enable/disable black hole.
  set dynamic-gateway { enable | disable } Enable use of dynamic gateway retrieved from a DHCP or PPP server.
  set virtual-wan-link { enable | disable } Enable/disable egress through the virtual-wan-link.
  set dstaddr { string } Name of firewall address or address group. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
  set internet-service { integer } Application ID in the Internet service database. range[0-4294967295] - datasource(s): firewall.internet-
service.id
  set internet-service-custom { string } Application name in the Internet service custom database. size[64] - datasource(s): fire-
wall.internet-service-custom.name
  set link-monitor-exempt { enable | disable } Enable/disable withdrawing this route when link monitor or health check is down.
  next
end

config router static6
  edit { seq-num }
  # Configure IPv6 static routing tables.
  set seq-num { integer } Sequence number. range[0-4294967295]
  set status { enable | disable } Enable/disable this static route.
  set dst { ipv6 network } Destination IPv6 prefix.
  set gateway { ipv6 address } IPv6 address of the gateway.
  set device { string } Gateway out interface or tunnel. size[35] - datasource(s): system.interface.name
  set devindex { integer } Device index (0 - 4294967295). range[0-4294967295]

```

```
    set distance { integer }  Administrative distance (1 - 255). range[1-255]
    set priority { integer }  Administrative priority (0 - 4294967295). range[0-4294967295]
    set comment { string }    Optional comments. size[255]
    set blackhole { enable | disable }  Enable/disable black hole.
  next
end
```


spamfilter

Introduction.

This section includes syntax for the following commands:

- `spamfilter bwl`
- `spamfilter bword`
- `spamfilter dnsbl`
- `spamfilter fortishield`
- `spamfilter iptrust`
- `spamfilter mheader`
- `spamfilter options`
- `spamfilter profile`

spamfilter bwl

Introduction.

```
config spamfilter bwl
  edit { id }
  # Configure anti-spam black/white list.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { id }
    # Anti-spam black/white list entries.
    set status { enable | disable } Enable/disable status.
    set id { integer } Entry ID. range[0-4294967295]
    set type { ip | email } Entry type.
      ip By IP address.
      email By email address.
    set action { reject | spam | clear } Reject, mark as spam or good email.
      reject Reject the connection.
      spam Mark as spam email.
      clear Mark as good email.
    set addr-type { ipv4 | ipv6 } IP address type.
      ipv4 IPv4 Address type.
      ipv6 IPv6 Address type.
    set ip4-subnet { ipv4 classnet } IPv4 network address/subnet mask bits.
    set ip6-subnet { ipv6 network } IPv6 network address/subnet mask bits.
    set pattern-type { wildcard | regexp } Wildcard pattern or regular expression.
      wildcard Wildcard pattern.
      regexp Perl regular expression.
    set email-pattern { string } Email address pattern. size[127]
  next
next
end
```

spamfilter bword

Introduction.

```
config spamfilter bword
  edit { id }
  # Configure AntiSpam banned word list.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
config entries
  edit { id }
  # Spam filter banned word.
  set status { enable | disable } Enable/disable status.
  set id { integer } Banned word entry ID. range[0-4294967295]
  set pattern { string } Pattern for the banned word. size[127]
  set pattern-type { wildcard | regexp } Wildcard pattern or regular expression.
    wildcard Wildcard pattern.
    regexp Perl regular expression.
  set action { spam | clear } Mark spam or good.
    spam Mark as spam email.
    clear Mark as good email.
  set where { subject | body | all } Component of the email to be scanned.
    subject Banned word in email subject.
    body Banned word in email body.
    all Banned word in both subject and body.
  set language { option } Language for the banned word.
    western Western.
    simch Simplified Chinese.
    trach Traditional Chinese.
    japanese Japanese.
    korean Korean.
    french French.
    thai Thai.
    spanish Spanish.
  set score { integer } Score value. range[1-99999]
next
next
```

end

spamfilter dnsbl

Introduction.

```
config spamfilter dnsbl
  edit { id }
  # Configure AntiSpam DNSBL/ORBL.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { id }
    # Spam filter DNSBL and ORBL server.
    set status { enable | disable } Enable/disable status.
    set id { integer } DNSBL/ORBL entry ID. range[0-4294967295]
    set server { string } DNSBL or ORBL server name. size[127]
    set action { reject | spam } Reject connection or mark as spam email.
      reject Reject the connection.
      spam Mark as spam email.
    next
  next
end
```

spamfilter fortishield

Introduction.

```
config spamfilter fortishield
  set spam-submit-srv { string }  Hostname of the spam submission server. size[63]
  set spam-submit-force { enable | disable }  Enable/disable force insertion of a new mime entity for the submission text.
  set spam-submit-txt2htm { enable | disable }  Enable/disable conversion of text email to HTML email.
end
```

spamfilter iptrust

Introduction.

```
config spamfilter iptrust
  edit { id }
  # Configure AntiSpam IP trust.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { id }
    # Spam filter trusted IP addresses.
    set status { enable | disable } Enable/disable status.
    set id { integer } Trusted IP entry ID. range[0-4294967295]
    set addr-type { ipv4 | ipv6 } Type of address.
      ipv4 IPv4 Address type.
      ipv6 IPv6 Address type.
    set ip4-subnet { ipv4 classnet } IPv4 network address or network address/subnet mask bits.
    set ip6-subnet { ipv6 network } IPv6 network address/subnet mask bits.
  next
next
end
```

spamfilter mheader

Introduction.

```
config spamfilter mheader
  edit { id }
  # Configure AntiSpam MIME header.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { id }
    # Spam filter mime header content.
    set status { enable | disable } Enable/disable status.
    set id { integer } Mime header entry ID. range[0-4294967295]
    set fieldname { string } Pattern for header field name. size[63]
    set fieldbody { string } Pattern for the header field body. size[127]
    set pattern-type { wildcard | regexp } Wildcard pattern or regular expression.
      wildcard Wildcard pattern.
      regexp Perl regular expression.
    set action { spam | clear } Mark spam or good.
      spam Mark as spam email.
      clear Mark as good email.
  next
next
end
```


spamfilter options

Introduction.

```
config spamfilter options
  set dns-timeout { integer }  DNS query time out (1 - 30 sec). range[1-30]
end
```

spamfilter profile

Introduction.

```
config spamfilter profile
edit { name }
# Configure AntiSpam profiles.
set name { string } Profile name. size[35]
set comment { string } Comment. size[255]
set flow-based { enable | disable } Enable/disable flow-based spam filtering.
set replacemsg-group { string } Replacement message group. size[35] - datasource(s): system.replacemsg-group.name
set spam-log { disable | enable } Enable/disable spam logging for email filtering.
set spam-log-fortiguard-response { disable | enable } Enable/disable logging FortiGuard spam response.
set spam-filtering { enable | disable } Enable/disable spam filtering.
set external { enable | disable } Enable/disable external Email inspection.
set options { option } Options.
    bannedword Content block.
    spambwl Black/white list.
    spamfsip Email IP address FortiGuard AntiSpam black list check.
    spamfssubmit Add FortiGuard AntiSpam spam submission text.
    spamfschksum Email checksum FortiGuard AntiSpam check.
    spamfsurl Email content URL FortiGuard AntiSpam check.
    spamhelodns Email helo/ehlo domain DNS check.
    spamraddrdns Email return address DNS check.
    spamrbl Email DNSBL & ORBL check.
    spamhdrcheck Email mime header check.
    spamfphish Email content phishing URL FortiGuard AntiSpam check.
set log { enable | disable } Enable/disable logging.
set action { pass | tag } Action for spam email.
    pass Allow spam email to pass through.
    tag Tag spam email with configured text in subject or header.
set tag-type { subject | header | spaminfo } Tag subject or header for spam email.
    subject Prepend text to spam email subject.
    header Append a user defined mime header to spam email.
    spaminfo Append spam info to spam email header.
set tag-msg { string } Subject text or header added to spam email. size[63]
set log { enable | disable } Enable/disable logging.
set action { pass | tag } Action for spam email.
    pass Allow spam email to pass through.
```

```
        tag    Tag spam email with configured text in subject or header.
set tag-type { subject | header | spaminfo }  Tag subject or header for spam email.
    subject  Prepend text to spam email subject.
    header   Append a user defined mime header to spam email.
    spaminfo Append spam info to spam email header.
set tag-msg { string }  Subject text or header added to spam email. size[63]
set log { enable | disable }  Enable/disable logging.
set action { pass | tag | discard }  Action for spam email.
    pass    Allow spam email to pass through.
    tag     Tag spam email with configured text in subject or header.
    discard Discard (block) spam email.
set tag-type { subject | header | spaminfo }  Tag subject or header for spam email.
    subject  Prepend text to spam email subject.
    header   Append a user defined mime header to spam email.
    spaminfo Append spam info to spam email header.
set tag-msg { string }  Subject text or header added to spam email. size[63]
set hdrop { disable | enable }  Enable/disable SMTP email header IP checks for spamfsip, spamrbl and spambwl filters.
set local-override { disable | enable }  Enable/disable local filter to override SMTP remote check result.
set log { enable | disable }  Enable/disable logging.
set action { pass | discard }  Action for spam email.
    pass    Allow spam email to pass through.
    discard Discard (block) spam email.
set log { enable | disable }  Enable/disable logging.
set log { enable | disable }  Enable/disable logging.
set log { enable | disable }  Enable/disable logging.
set spam-bword-threshold { integer }  Spam banned word threshold. range[0-2147483647]
set spam-bword-table { integer }  Anti-spam banned word table ID. range[0-4294967295] - datasource(s): spamfilter.bword.id
set spam-bwl-table { integer }  Anti-spam black/white list table ID. range[0-4294967295] - datasource(s): spamfilter.bwl.id
set spam-mheader-table { integer }  Anti-spam MIME header table ID. range[0-4294967295] - datasource(s): spamfilter.mheader.id
set spam-rbl-table { integer }  Anti-spam DNSBL table ID. range[0-4294967295] - datasource(s): spamfilter.dnsbl.id
set spam-iptrust-table { integer }  Anti-spam IP trust table ID. range[0-4294967295] - datasource(s): spamfilter.iptrust.id
next
end
```

switch-controller

Use switch-controller commands to configure a host of options related to managing an external FortiSwitch unit.

This section includes syntax for the following commands:

- `switch-controller 802-1X-settings`
- `switch-controller custom-command`
- `switch-controller global`
- `switch-controller igmp-snooping`
- `switch-controller lldp-profile`
- `switch-controller lldp-settings`
- `switch-controller mac-sync-settings`
- `switch-controller managed-switch`
- `switch-controller qos dot1p-map`
- `switch-controller qos ip-dscp-map`
- `switch-controller qos qos-policy`
- `switch-controller qos queue-policy`
- `switch-controller quarantine`
- `switch-controller security-policy 802-1X`
- `switch-controller security-policy captive-portal`
- `switch-controller storm-control`
- `switch-controller stp-settings`
- `switch-controller switch-group`
- `switch-controller switch-log`
- `switch-controller switch-profile`
- `switch-controller vlan`

switch-controller 802-1X-settings

Introduction.

```
config switch-controller 802-1X-settings
  set link-down-auth { set-unauth | no-action }  Authentication state to set if a link is down.
    set-unauth  Interface set to unauth when down. Reauthentication is needed.
    no-action   Interface reauthentication is not needed.
  set reauth-period { integer }  Reauthentication time interval (1 - 1440 sec, default = 60). range[1-1440]
  set max-reauth-attempt { integer }  Maximum number of authentication attempts (0 - 15, default = 3). range[0-15]
end
```

switch-controller custom-command

Introduction.

```
config switch-controller custom-command
  edit { command-name }
  # Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices.
  set command-name { string }  Command name called by the FortiGate switch controller in the execute command. size[35]
  set description { string }  Description. size[35]
  set command { string }  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). size[255]
  next
end
```

switch-controller global

Introduction.

```
config switch-controller global
    set mac-aging-interval { integer }    Time after which an inactive MAC is aged out (10 - 1000000 sec, default = 300, 0 = disable). range[10-1000000]
    set allow-multiple-interfaces { enable | disable }    Enable/disable multiple FortiLink interfaces for redundant connections between a managed FortiSwitch and FortiGate.
    config disable-discovery
        edit { name }
            # Prevent this FortiSwitch from discovering.
            set name { string }    Managed device ID. size[64]
        next
    end
```

switch-controller igmp-snooping

Introduction.

```
config switch-controller igmp-snooping
    set aging-time { integer }    Maximum number of seconds to retain a multicast snooping entry for which no packets have been seen (15 - 3600 sec,
default = 300). range[15-3600]
    set flood-unknown-multicast { enable | disable }    Enable/disable unknown multicast flooding.
end
```


switch-controller lldp-profile

Introduction.

```

config switch-controller lldp-profile
  edit { name }
  # Configure FortiSwitch LLDP profiles.
  set name { string } Profile name. size[63]
  set med-tlvs { inventory-management | network-policy } Transmitted LLDP-MED TLVs (type-length-value descriptions): inventory management TLV
  and/or network policy TLV.
  inventory-management Inventory management TLV.
  network-policy Network policy TLVS.
  set 802.1-tlvs { port-vlan-id } Transmitted IEEE 802.1 TLVs.
  port-vlan-id Port native VLAN TLV.
  set 802.3-tlvs { max-frame-size } Transmitted IEEE 802.3 TLVs.
  max-frame-size Maximum frame size TLV.
  set auto-isl { disable | enable } Enable/disable auto inter-switch LAG.
  set auto-isl-hello-timer { integer } Auto inter-switch LAG hello timer duration (1 - 30 sec, default = 3). range[1-30]
  set auto-isl-receive-timeout { integer } Auto inter-switch LAG timeout if no response is received (3 - 90 sec, default = 9). range[3-90]
  set auto-isl-port-group { integer } Auto inter-switch LAG port group ID (0 - 9). range[0-9]
  config med-network-policy
    edit { name }
    # Configuration method to edit Media Endpoint Discovery (MED) network policy type-length-value (TLV) categories.
    set name { string } Policy type name. size[63]
    set status { disable | enable } Enable or disable this TLV.
    set vlan { integer } ID of VLAN to advertise, if configured on port (0 - 4094, 0 = priority tag). range[0-4094]
    set priority { integer } Advertised Layer 2 priority (0 - 7; from lowest to highest priority). range[0-7]
    set dscp { integer } Advertised Differentiated Services Code Point (DSCP) value, a packet header value indicating the level of ser-
  vice requested for traffic, such as high priority or best effort delivery. range[0-63]
    next
  config custom-tlvs
    edit { name }
    # Configuration method to edit custom TLV entries.
    set name { string } TLV name (not sent). size[63]
    set oui { string } Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.
    set subtype { integer } Organizationally defined subtype (0 - 255). range[0-255]
    set information-string { string } Organizationally defined information string (0 - 507 hexadecimal bytes).
    next
  next

```

end

switch-controller lldp-settings

Introduction.

```
config switch-controller lldp-settings
    set status { enable | disable }    Enable/disable LLDP global settings.
    set tx-hold { integer }    Number of tx-intervals before local LLDP data expires (1 - 16, default = 4). Packet TTL is tx-hold * tx-interval. range
[1-16]
    set tx-interval { integer }    Frequency of LLDP PDU transmission from FortiSwitch (5 - 4095 sec, default = 30). Packet TTL is tx-hold * tx-inter-
val. range[5-4095]
    set fast-start-interval { integer }    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). range[0-255]
    set management-interface { internal | mgmt }    Primary management interface to be advertised in LLDP and CDP PDUs.
        internal    Use internal interface.
        mgmt        Use management interface.
end
```

switch-controller mac-sync-settings

Introduction.

```
config switch-controller mac-sync-settings
    set mac-sync-interval { integer }    Time interval between MAC synchronizations (30 - 600 sec, default = 60, 0 = disable MAC synchronization).
    range[30-600]
end
```

switch-controller managed-switch

Introduction.

```

config switch-controller managed-switch
  edit { switch-id }
  # Configure FortiSwitch devices that are managed by this FortiGate.
  set switch-id { string }   Managed-switch id. size[16]
  set name { string }       Managed-switch name. size[35]
  set description { string } Description. size[63]
  set switch-profile { string } FortiSwitch profile. size[35] - datasource(s): switch-controller.switch-profile.name
  set fsw-wan1-peer { string } Fortiswitch WAN1 peer port. size[35]
  set fsw-wan1-admin { discovered | disable | enable } FortiSwitch WAN1 admin status; enable to authorize the FortiSwitch as a managed
switch.
  set fsw-wan2-peer { string } FortiSwitch WAN2 peer port. size[35]
  set fsw-wan2-admin { discovered | disable | enable } FortiSwitch WAN2 admin status; enable to authorize the FortiSwitch as a managed
switch.
  set poe-pre-standard-detection { enable | disable } Enable/disable PoE pre-standard detection.
  set directly-connected { integer } Directly connected FortiSwitch. range[0-1]
  set connected { integer } CAPWAP connection. range[0-255]
  set version { integer } FortiSwitch version. range[0-255]
  set max-allowed-trunk-members { integer } FortiSwitch maximum allowed trunk members. range[0-255]
  set pre-provisioned { integer } Pre-provisioned managed switch. range[0-255]
  set dynamic-capability { integer } List of features this FortiSwitch supports (not configurable) that is sent to the FortiGate device for
subsequent configuration initiated by the FortiGate device. range[0-4294967295]
  set switch-device-tag { string } User definable label/tag. size[32]
  set dynamically-discovered { integer } Dynamically discovered FortiSwitch. range[0-1]
  set staged-image-version { string } Staged image version for FortiSwitch. size[127]
  set delayed-restart-trigger { integer } Delayed restart triggered for this FortiSwitch. range[0-255]
config ports
  edit { port-name }
  # Managed-switch port list.
  set port-name { string } Switch port name. size[15]
  set port-owner { string } Switch port name. size[15]
  set switch-id { string } Switch id. size[16]
  set speed { option } Switch port speed; default and available settings depend on hardware.
    10half      10M half-duplex.
    10full      10M full-duplex.
    100half     100M half-duplex.

```

```

    100full      100M full-duplex.
    1000auto    Auto-negotiation (1G full-duplex only).
    1000fiber   1G full-duplex (fiber SFPs only)
    1000full    1G full-duplex
    10000       10G full-duplex
    40000       40G full-duplex
    auto        Auto-negotiation.
    auto-module Auto Module.
set speed-mask { integer } Switch port speed mask. range[0-4294967295]
set status { up | down } Switch port admin status: up or down.
    up        Set admin status up.
    down      Set admin status down.
set poe-status { enable | disable } Enable/disable PoE status.
set poe-pre-standard-detection { enable | disable } Enable/disable PoE pre-standard detection.
set port-number { integer } Port number. range[1-64]
set port-prefix-type { integer } Port prefix type. range[0-1]
set fortilink-port { integer } FortiLink uplink port. range[0-1]
set poe-capable { integer } PoE capable. range[0-1]
set stacking-port { integer } Stacking port. range[0-1]
set fiber-port { integer } Fiber-port. range[0-1]
set flags { integer } Port properties flags. range[0-4294967295]
set isl-local-trunk-name { string } ISL local trunk name. size[15]
set isl-peer-port-name { string } ISL peer port name. size[15]
set isl-peer-device-name { string } ISL peer device name. size[16]
set fgt-peer-port-name { string } FGT peer port name. size[15]
set fgt-peer-device-name { string } FGT peer device name. size[16]
set vlan { string } Assign switch ports to a VLAN. size[15] - datasource(s): system.interface.name
set allowed-vlans-all { enable | disable } Enable/disable all defined vlans on this port.
config allowed-vlans
    edit { vlan-name }
        # Configure switch port tagged vlans
        set vlan-name { string } VLAN name. size[79] - datasource(s): system.interface.name
    next
config untagged-vlans
    edit { vlan-name }
        # Configure switch port untagged vlans
        set vlan-name { string } VLAN name. size[79] - datasource(s): system.interface.name
    next
set type { physical | trunk } Interface type: physical or trunk port.
    physical Physical port.
    trunk     Trunk port.
set dhcp-snooping { untrusted | trusted } Trusted or untrusted DHCP-snooping interface.
    untrusted Untrusted DHCP snooping interface.

```

```

        trusted    Trusted DHCP snooping interface.
set dhcp-snoop-option82-trust { enable | disable }  Enable/disable allowance of DHCP with option-82 on untrusted interface.
set igmp-snooping { enable | disable }  Set IGMP snooping mode for the physical port interface.
set igmps-flood-reports { enable | disable }  Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.
set igmps-flood-traffic { enable | disable }  Enable/disable flooding of IGMP snooping traffic to this interface.
set stp-state { enabled | disabled }  Enable/disable Spanning Tree Protocol (STP) on this interface.
        enabled  Enable STP on this interface.
        disabled Disable STP on this interface.
set stp-root-guard { enabled | disabled }  Enable/disable STP root guard on this interface.
        enabled  Enable STP root-guard on this interface.
        disabled Disable STP root-guard on this interface.
set stp-bpdu-guard { enabled | disabled }  Enable/disable STP BPDU guard on this interface.
        enabled  Enable STP BPDU guard on this interface.
        disabled Disable STP BPDU guard on this interface.
set stp-bpdu-guard-timeout { integer }  BPDU Guard disabling protection (0 - 120 min). range[0-120]
set edge-port { enable | disable }  Enable/disable this interface as an edge port, bridging connections between workstations and/or
computers.
set loop-guard { enabled | disabled }  Enable/disable loop-guard on this interface, an STP optimization used to prevent network
loops.
        enabled  Enable loop-guard on this interface.
        disabled Disable loop-guard on this interface.
set loop-guard-timeout { integer }  Loop-guard timeout (0 - 120 min, default = 45). range[0-120]
set qos-policy { string }  Switch controller QoS policy from available options. size[63] - datasource(s): switch-controller.qos.qos-
policy.name
set port-security-policy { string }  Switch controller authentication policy to apply to this managed switch from available options.
size[31] - datasource(s): switch-controller.security-policy.802-1X.name,switch-controller.security-policy.captive-portal.name
set lldp-status { disable | rx-only | tx-only | tx-rx }  LLDP transmit and receive status.
        disable Disable LLDP TX and RX.
        rx-only  Enable LLDP as RX only.
        tx-only  Enable LLDP as TX only.
        tx-rx   Enable LLDP TX and RX.
set lldp-profile { string }  LLDP port TLV profile. size[63] - datasource(s): switch-controller.lldp-profile.name
set port-selection-criteria { option }  Algorithm for aggregate port selection.
        src-mac    Source MAC address.
        dst-mac    Destination MAC address.
        src-dst-mac Source and destination MAC address.
        src-ip     Source IP address.
        dst-ip     Destination IP address.
        src-dst-ip Source and destination IP address.
set description { string }  Description for port. size[63]
set lacp-speed { slow | fast }  end Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second
(fast).
        slow  Send LACP message every 30 seconds.

```

```

        fast Send LACP message every second.
    set mode { static | lacp-passive | lacp-active } LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.
        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.
    set bundle { enable | disable } Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.
    set member-withdrawal-behavior { forward | block } Port behavior after it withdraws because of loss of control packets.
        forward Forward traffic.
        block Block traffic.
    set mclag { enable | disable } Enable/disable multi-chassis link aggregation (MCLAG).
    set min-bundle { integer } Minimum size of LAG bundle (1 - 24, default = 1) range[1-24]
    set max-bundle { integer } Maximum size of LAG bundle (1 - 24, default = 24) range[1-24]
    config members
        edit { member-name }
            # Aggregated LAG bundle interfaces.
            set member-name { string } Interface name from available options. size[64]
        next
    next
    set local-override { enable | disable } Enable to configure local STP settings that override global STP settings.
    set name { string } Name of local STP settings configuration. size[31]
    set status { enable | disable } Enable/disable STP.
    set revision { integer } STP revision number (0 - 65535). range[0-65535]
    set hello-time { integer } Period of time between successive STP frame Bridge Protocol Data Units (BPDUs) sent on a port (1 - 10 sec, default = 2). range[1-10]
    set forward-time { integer } Period of time a port is in listening and learning state (4 - 30 sec, default = 15). range[4-30]
    set max-age { integer } Maximum time before a bridge port saves its configuration BPDUs information (6 - 40 sec, default = 20). range[6-40]

    set max-hops { integer } Maximum number of hops between the root bridge and the furthest bridge (1- 40, default = 20). range[1-40]
    set pending-timer { integer } Pending time (1 - 15 sec, default = 4). range[1-15]
    set status { enable | disable } Enable/disable STP.
    set local-override { enable | disable } Enable to configure local logging settings that override global logging settings.
    set status { enable | disable } Enable/disable adding FortiSwitch logs to the FortiGate event log.
    set severity { option } Severity of FortiSwitch logs that are added to the FortiGate event log.
        emergency Emergency level.
        alert Alert level.
        critical Critical level.
        error Error level.
        warning Warning level.
        notification Notification level.
        information Information level.
        debug Debug level.
    set local-override { enable | disable } Enable to override global FortiSwitch storm control settings for this FortiSwitch.

```



```
    set rate { integer } 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. range[1-10000000]
    set unknown-unicast { enable | disable } Enable/disable storm control to drop unknown unicast traffic.
    set unknown-multicast { enable | disable } Enable/disable storm control to drop unknown multicast traffic.
    set broadcast { enable | disable } Enable/disable storm control to drop broadcast traffic.
config custom-command
  edit { command-entry }
    # Configuration method to edit FortiSwitch commands to be pushed to this FortiSwitch device upon rebooting the FortiGate switch con-
troller or the FortiSwitch.
    set command-entry { string } List of FortiSwitch commands. size[35]
    set command-name { string } Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller
custom-command. size[35] - datasource(s): switch-controller.custom-command.command-name
  next
  set local-override { enable | disable } Enable/disable overriding the global IGMP snooping configuration.
  set aging-time { integer } Maximum time to retain a multicast snooping entry for which no packets have been seen (15 - 3600 sec,
default = 300). range[15-3600]
  set flood-unknown-multicast { enable | disable } Enable/disable unknown multicast flooding.
  set local-override { enable | disable } Enable to override global 802.1X settings on individual FortiSwitches.
  set link-down-auth { set-unauth | no-action } Interface-reauthentication state to set if a link is down.
    set-unauth Interface set to unauth when down. Reauthentication is needed.
    no-action Interface reauthentication is not needed.
  set reauth-period { integer } Period of time to allow for reauthentication (1 - 1440 sec, default = 60, 0 = disable reauthentication).
range[1-1440]
  set max-reauth-attempt { integer } Maximum number of authentication attempts (0 - 15, default = 3). range[0-15]
  next
end
```

switch-controller qos dot1p-map

Introduction.

```
config switch-controller qos dot1p-map
edit { name }
# Configure FortiSwitch QoS 802.1p.
set name { string } Dot1p map name. size[63]
set description { string } Description of the 802.1p name. size[63]
set priority-0 { option } COS queue mapped to dot1p priority number.
    queue-0 COS queue 0.
    queue-1 COS queue 1.
    queue-2 COS queue 2.
    queue-3 COS queue 3.
    queue-4 COS queue 4.
    queue-5 COS queue 5.
    queue-6 COS queue 6.
    queue-7 COS queue 7.
set priority-1 { option } COS queue mapped to dot1p priority number.
    queue-0 COS queue 0.
    queue-1 COS queue 1.
    queue-2 COS queue 2.
    queue-3 COS queue 3.
    queue-4 COS queue 4.
    queue-5 COS queue 5.
    queue-6 COS queue 6.
    queue-7 COS queue 7.
set priority-2 { option } COS queue mapped to dot1p priority number.
    queue-0 COS queue 0.
    queue-1 COS queue 1.
    queue-2 COS queue 2.
    queue-3 COS queue 3.
    queue-4 COS queue 4.
    queue-5 COS queue 5.
    queue-6 COS queue 6.
    queue-7 COS queue 7.
set priority-3 { option } COS queue mapped to dot1p priority number.
    queue-0 COS queue 0.
    queue-1 COS queue 1.
```

```
queue-2 COS queue 2.
queue-3 COS queue 3.
queue-4 COS queue 4.
queue-5 COS queue 5.
queue-6 COS queue 6.
queue-7 COS queue 7.
set priority-4 { option } COS queue mapped to dot1p priority number.
queue-0 COS queue 0.
queue-1 COS queue 1.
queue-2 COS queue 2.
queue-3 COS queue 3.
queue-4 COS queue 4.
queue-5 COS queue 5.
queue-6 COS queue 6.
queue-7 COS queue 7.
set priority-5 { option } COS queue mapped to dot1p priority number.
queue-0 COS queue 0.
queue-1 COS queue 1.
queue-2 COS queue 2.
queue-3 COS queue 3.
queue-4 COS queue 4.
queue-5 COS queue 5.
queue-6 COS queue 6.
queue-7 COS queue 7.
set priority-6 { option } COS queue mapped to dot1p priority number.
queue-0 COS queue 0.
queue-1 COS queue 1.
queue-2 COS queue 2.
queue-3 COS queue 3.
queue-4 COS queue 4.
queue-5 COS queue 5.
queue-6 COS queue 6.
queue-7 COS queue 7.
set priority-7 { option } COS queue mapped to dot1p priority number.
queue-0 COS queue 0.
queue-1 COS queue 1.
queue-2 COS queue 2.
queue-3 COS queue 3.
queue-4 COS queue 4.
queue-5 COS queue 5.
queue-6 COS queue 6.
queue-7 COS queue 7.
next
```

end

switch-controller qos ip-dscp-map

Introduction.

```
config switch-controller qos ip-dscp-map
  edit { name }
  # Configure FortiSwitch QoS IP precedence/DSCP.
  set name { string } Dscp map name. size[63]
  set description { string } Description of the ip-dscp map name. size[63]
  config map
    edit { name }
    # Maps between IP-DSCP value to COS queue.
    set name { string } Dscp mapping entry name. size[63]
    set cos-queue { integer } COS queue number. range[0-7]
    set diffserv { option } Differentiated service.
      CS0 DSCP CS0.
      CS1 DSCP CS1.
      AF11 DSCP AF11.
      AF12 DSCP AF12.
      AF13 DSCP AF13.
      CS2 DSCP CS2.
      AF21 DSCP AF21.
      AF22 DSCP AF22.
      AF23 DSCP AF23.
      CS3 DSCP CS3.
      AF31 DSCP AF31.
      AF32 DSCP AF32.
      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.
    set ip-precedence { option } IP Precedence.
      network-control Network control.
      internetwork-control Internetwork control.
```

```
        critic-ecp      Critic ECP.
        flashoverride   Flash override.
        flash           Flash.
        immediate       Immediate.
        priority        Priority.
        routine         Routine.
    set value { string } Raw values of DSCP (0 - 63).
next
end
```

switch-controller qos qos-policy

Introduction.

```
config switch-controller qos qos-policy
  edit { name }
  # Configure FortiSwitch QoS policy.
  set name { string }   QoS policy name. size[63]
  set default-cos { integer }   Default cos queue for untagged packets. range[0-7]
  set trust-dot1p-map { string }   QoS trust 802.1p map. size[63] - datasource(s): switch-controller.qos.dot1p-map.name
  set trust-ip-dscp-map { string }   QoS trust ip dscp map. size[63] - datasource(s): switch-controller.qos.ip-dscp-map.name
  set queue-policy { string }   QoS egress queue policy. size[63] - datasource(s): switch-controller.qos.queue-policy.name
  next
end
```

switch-controller qos queue-policy

Introduction.

```
config switch-controller qos queue-policy
  edit { name }
  # Configure FortiSwitch QoS egress queue policy.
  set name { string }  QoS policy name size[63]
  set schedule { strict | round-robin | weighted }  COS queue scheduling.
    strict      Strict scheduling.
    round-robin Round robin scheduling.
    weighted    Weighted round robin scheduling.
  config cos-queue
    edit { name }
    # COS queue configuration.
    set name { string }  Cos queue ID. size[63]
    set description { string }  Description of the COS queue. size[63]
    set min-rate { integer }  Minimum rate (kbps). 0 to disable. range[0-4294967295]
    set max-rate { integer }  Maximum rate (kbps). 0 to disable. range[0-4294967295]
    set drop-policy { taildrop | weighted-random-early-detection }  COS queue drop policy.
      taildrop      Taildrop policy.
      weighted-random-early-detection  Weighted random early detection drop policy.
    set weight { integer }  Weight of weighted round robin scheduling. range[0-4294967295]
  next
next
end
```


switch-controller quarantine

Introduction.

```
config switch-controller quarantine
  set quarantine { enable | disable }  Enable/disable quarantine.
  config targets
    edit { mac }
      # Quarantine MACs.
      set mac { mac address }  Quarantine MAC.
      set entry-id { integer }  FSW entry id for the quarantine MAC. range[0-4294967295]
      set description { string }  Description for the quarantine MAC. size[63]
    config tag
      edit { tags }
        # Tags for the quarantine MAC.
        set tags { string }  Tag string(eg. string1 string2 string3). size[63]
      next
    next
  end
```

switch-controller security-policy 802-1X

Introduction.

```
config switch-controller security-policy 802-1X
  edit { name }
  # Configure 802.1X MAC Authentication Bypass (MAB) policies.
  set name { string } Policy name. size[31]
  set security-mode { 802.1X | 802.1X-mac-based } Port or MAC based 802.1X security mode.
    802.1X      802.1X port based authentication.
    802.1X-mac-based 802.1X MAC based authentication.
  config user-group
    edit { name }
    # Name of user-group to assign to this MAC Authentication Bypass (MAB) policy.
    set name { string } Group name. size[64] - datasource(s): user.group.name
    next
  set mac-auth-bypass { disable | enable } Enable/disable MAB for this policy.
  set eap-passthru { disable | enable } Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for
more flexible authentication.
  set guest-vlan { disable | enable } Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.
  set guest-vlanid { integer } Guest VLAN ID. range[0-65535]
  set guest-vlan-id { string } Guest VLAN name. size[15] - datasource(s): system.interface.name
  set guest-auth-delay { integer } Guest authentication delay (60 - 900 sec, default = 120). range[60-900]
  set auth-fail-vlan { disable | enable } Enable to allow limited access to clients that cannot authenticate.
  set auth-fail-vlanid { integer } VLAN ID on which authentication failed. range[0-65535]
  set auth-fail-vlan-id { string } VLAN ID on which authentication failed. size[15] - datasource(s): system.interface.name
  set radius-timeout-overwrite { disable | enable } Enable to override the global RADIUS session timeout.
  set policy-type { 802.1X } Policy type.
    802.1X 802.1X security policy.
  next
end
```

switch-controller security-policy captive-portal

Introduction.

```
config switch-controller security-policy captive-portal
  edit { name }
  # Names of VLANs that use captive portal authentication.
  set name { string } Policy name. size[31]
  set vlan { string } Names of VLANs that use captive portal authentication. size[15] - datasource(s): system.interface.name
  set policy-type { captive-portal } Policy type.
    captive-portal Captive portal security policy.
  next
end
```

switch-controller storm-control

Introduction.

```
config switch-controller storm-control
    set rate { integer } 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. range[1-10000000]
    set unknown-unicast { enable | disable } Enable/disable storm control to drop unknown unicast traffic.
    set unknown-multicast { enable | disable } Enable/disable storm control to drop unknown multicast traffic.
    set broadcast { enable | disable } Enable/disable storm control to drop broadcast traffic.
end
```

switch-controller stp-settings

Introduction.

```
config switch-controller stp-settings
  set name { string }  Name of global STP settings configuration. size[31]
  set status { enable | disable }  Enable/disable STP.
  set revision { integer }  STP revision number (0 - 65535). range[0-65535]
  set hello-time { integer }  Period of time between successive STP frame Bridge Protocol Data Units (BPDUs) sent on a port (1 - 10 sec, default = 2). range[1-10]
  set forward-time { integer }  Period of time a port is in listening and learning state (4 - 30 sec, default = 15). range[4-30]
  set max-age { integer }  Maximum time before a bridge port saves its configuration BPDU information (6 - 40 sec, default = 20). range[6-40]
  set max-hops { integer }  Maximum number of hops between the root bridge and the furthest bridge (1- 40, default = 20). range[1-40]
  set pending-timer { integer }  Pending time (1 - 15 sec, default = 4). range[1-15]
end
```

switch-controller switch-group

Introduction.

```
config switch-controller switch-group
  edit { name }
  # Configure FortiSwitch switch groups.
  set name { string }  Switch group name. size[35]
  set description { string }  Optional switch group description. size[63]
  config members
    edit { name }
    # FortiSwitch members belonging to this switch group.
    set name { string }  Managed device ID. size[64] - datasource(s): switch-controller.managed-switch.switch-id
  next
next
end
```

switch-controller switch-log

Introduction.

```
config switch-controller switch-log
  set status { enable | disable }  Enable/disable adding FortiSwitch logs to FortiGate event log.
  set severity { option }  Severity of FortiSwitch logs that are added to the FortiGate event log.
    emergency  Emergency level.
    alert      Alert level.
    critical   Critical level.
    error      Error level.
    warning    Warning level.
    notification Notification level.
    information Information level.
    debug      Debug level.
end
```

switch-controller switch-profile

Introduction.

```
config switch-controller switch-profile
  edit { name }
  # Configure FortiSwitch switch profile.
  set name { string } FortiSwitch Profile name. size[35]
  set login-passwd-override { enable | disable } Enable/disable overriding the admin administrator password for a managed FortiSwitch with
the FortiGate admin administrator account password.
  set login-passwd { password_string } Login password of managed FortiSwitch. size[64]
  next
end
```


switch-controller vlan

Introduction.

```
config switch-controller vlan
  edit { name }
  # Configure VLANs for switch controller.
  set name { string }   Switch VLAN name. size[15]
  set vdom { string }   Virtual domain, size[32]
  set vlanid { integer } VLAN ID. range[1-4094]
  set comments { string } Comment. size[63]
  set color { integer } Color of icon on the GUI. range[0-32]
  set security { open | captive-portal | 8021x } Security.
      open          Open.
      captive-portal Captive portal.
      8021x         802.1x
  set auth { radius | usergroup } Authentication.
      radius        RADIUS.
      usergroup     User group.
  set radius-server { string } Authentication radius server. size[35] - datasource(s): user.radius.name
  set usergroup { string } Authentication usergroup. size[35] - datasource(s): user.group.name
  set portal-message-override-group { string } Specify captive portal replacement message override group. size[35]
  set auth-disclaimer-page { string } Override auth-disclaimer-page message with message from portal-message-overrides group. size[35]
  set auth-reject-page { string } Override auth-reject-page message with message from portal-message-overrides group. size[35]
  set auth-login-page { string } Override auth-login-page message with message from portal-message-overrides group. size[35]
  set auth-login-failed-page { string } Override auth-login-failed-page message with message from portal-message-overrides group. size
[35]
config selected-usergroups
  edit { name }
  # Selected user group.
  set name { string } User group name. size[64] - datasource(s): user.group.name
  next
next
end
```

system

Use system commands to configure options related to the overall operation of your FortiGate.

This section includes syntax for the following commands:

- `system 3g-modem custom`
- `system accprofile`
- `system admin`
- `system alarm`
- `system alias`
- `system api-user`
- `system arp-table`
- `system auto-install`
- `system auto-script`
- `system autoupdate push-update`
- `system autoupdate schedule`
- `system autoupdate tunneling`
- `system central-management`
- `system cluster-sync`
- `system console`
- `system csf`
- `system custom-language`
- `system ddns`
- `system dedicated-mgmt`
- `system dhcp server | dhcp6 server`
- `system dns`
- `system dns-database`
- `system dns-server`
- `system dscp-based-priority`

-
- system email-server
 - system fips-cc
 - system fm
 - system fortiguard
 - system fortimanager
 - system fortisandbox
 - system fso-polling
 - system ftm-push
 - system geoup-override
 - system global
 - system gre-tunnel
 - system ha
 - system ha-monitor
 - system interface
 - system ipip-tunnel
 - system ips-urfilter-dns
 - system ipv6-neighbor-cache
 - system ipv6-tunnel
 - system link-monitor
 - system lte-modem
 - system mac-address-table
 - system management-tunnel
 - system mobile-tunnel
 - system modem
 - system nat64
 - system netflow
 - system network-visibility
 - system np6
 - system npu
 - system ntp
 - system object-tag

- system password-policy
- system password-policy-guest-admin
- system physical-switch
- system pppoe-interface
- system probe-response
- system proxy-arp
- system replacemsg admin
- system replacemsg alertmail
- system replacemsg auth
- system replacemsg device-detection-portal
- system replacemsg ec
- system replacemsg fortiguard-wf
- system replacemsg ftp
- system replacemsg http
- system replacemsg mail
- system replacemsg nac-quar
- system replacemsg nntp
- system replacemsg spam
- system replacemsg sslvpn
- system replacemsg traffic-quota
- system replacemsg utm
- system replacemsg webproxy
- system replacemsg-group
- system replacemsg-image
- system resource-limits
- system session-helper
- system session-ttl
- system settings
- system sflow
- system sit-tunnel
- system sms-server

- system snmp community
- system snmp sysinfo
- system snmp user
- system storage
- system stp
- system switch-interface
- system tos-based-priority
- system vdom
- system vdom-dns
- system vdom-link
- system vdom-netflow
- system vdom-property
- system vdom-radius-server
- system vdom-sflow
- system virtual-switch
- system virtual-wan-link
- system virtual-wire-pair
- system vxlan
- system wccp
- system wireless ap-status
- system wireless settings
- system zone

system 3g-modem custom

Introduction.

```
config system 3g-modem custom
  edit { id }
  # 3G MODEM custom.
  set id { integer } ID. range[0-4294967295]
  set vendor { string } MODEM vendor name. size[35]
  set model { string } MODEM model name. size[35]
  set vendor-id { string } USB vendor ID in hexadecimal format (0000-ffff).
  set product-id { string } USB product ID in hexadecimal format (0000-ffff).
  set class-id { string } USB interface class in hexadecimal format (00-ff).
  set init-string { string } Init string in hexadecimal format (even length). size[127]
next
end
```

system accprofile

Introduction.

```
config system accprofile
  edit { name }
  # Configure access profiles for system administrators.
  set name { string } Profile name. size[35]
  set scope { vdom | global } Scope of admin access: global or specific VDOM(s).
    vdom VDOM access.
    global Global access.
  set comments { string } Comment. size[255]
  set mntgrp { none | read | read-write } Administrator access to maintenance commands including reset to factory defaults, format log disk,
reboot, restore, and shutdown.
    none No access.
    read Read access.
    read-write Read/write access.
  set admingrp { none | read | read-write } Administrator access to add, remove, and edit admin accounts and access profiles.
    none No access.
    read Read access.
    read-write Read/write access.
  set updategrp { none | read | read-write } Administrator access to the FortiGuard configuration and requesting FortiGuard updates.
    none No access.
    read Read access.
    read-write Read/write access.
  set authgrp { none | read | read-write } Administrator access to Users and Devices.
    none No access.
    read Read access.
    read-write Read/write access.
  set sysgrp { none | read | read-write } Administrator access to System administration settings.
    none No access.
    read Read access.
    read-write Read/write access.
  set netgrp { none | read | read-write } Administrator access to Networking settings.
    none No access.
    read Read access.
    read-write Read/write access.
  set loggrp { none | read | read-write | custom } Administrator access to Logging and Reporting including viewing log messages.
    none No access.
```

```

    read      Read access.
    read-write Read/write access.
    custom    Customized access.
set routegrp { none | read | read-write } Administrator access to the Routing configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set fwgrp { none | read | read-write | custom } Administrator access to the Firewall configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
    custom    Customized access.
set vpngrp { none | read | read-write } Administrator access to IPsec, SSL, PPTP, and L2TP VPN.
    none      No access.
    read      Read access.
    read-write Read/write access.
set utmgrp { none | read | read-write | custom } Administrator access to Security Profiles.
    none      No access.
    read      Read access.
    read-write Read/write access.
    custom    Customized access.
set wanoptgrp { none | read | read-write } Administrator access to WAN Opt & Cache.
    none      No access.
    read      Read access.
    read-write Read/write access.
set endpoint-control-grp { none | read | read-write } Administrator access to Endpoint Control.
    none      No access.
    read      Read access.
    read-write Read/write access.
set wifi { none | read | read-write } Administrator access to the WiFi controller and Switch controller.
    none      No access.
    read      Read access.
    read-write Read/write access.
set policy { none | read | read-write } Policy Configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set address { none | read | read-write } Address Configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set service { none | read | read-write } Service Configuration.
    none      No access.
```



```
    read      Read access.
    read-write Read/write access.
set schedule { none | read | read-write }  Schedule Configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set packet-capture { none | read | read-write }  Packet Capture configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set others { none | read | read-write }  Other firewall configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set config { none | read | read-write }  Log & Report configuration.
    none      No access.
    read      Read access.
    read-write Read/write access.
set data-access { none | read | read-write }  Log & Report Data Access.
    none      No access.
    read      Read access.
    read-write Read/write access.
set report-access { none | read | read-write }  Log & Report Report Access.
    none      No access.
    read      Read access.
    read-write Read/write access.
set threat-weight { none | read | read-write }  Log & Report Threat Weight.
    none      No access.
    read      Read access.
    read-write Read/write access.
set antivirus { none | read | read-write }  Antivirus profiles and settings.
    none      No access.
    read      Read access.
    read-write Read/write access.
set ips { none | read | read-write }  IPS profiles and settings.
    none      No access.
    read      Read access.
    read-write Read/write access.
set webfilter { none | read | read-write }  Web Filter profiles and settings.
    none      No access.
    read      Read access.
    read-write Read/write access.
set spamfilter { none | read | read-write }  AntiSpam filter and settings.
```

```
        none      No access.
        read      Read access.
        read-write Read/write access.
set data-loss-prevention { none | read | read-write }  DLP profiles and settings.
        none      No access.
        read      Read access.
        read-write Read/write access.
set application-control { none | read | read-write }  Application Control profiles and settings.
        none      No access.
        read      Read access.
        read-write Read/write access.
set icap { none | read | read-write }  ICAP profiles and settings.
        none      No access.
        read      Read access.
        read-write Read/write access.
set voip { none | read | read-write }  VoIP profiles and settings.
        none      No access.
        read      Read access.
        read-write Read/write access.
set waf { none | read | read-write }  Web Application Firewall profiles and settings.
        none      No access.
        read      Read access.
        read-write Read/write access.
set dnsfilter { none | read | read-write }  DNS Filter profiles and settings.
        none      No access.
        read      Read access.
        read-write Read/write access.
set admintimeout-override { enable | disable }  Enable/disable overriding the global administrator idle timeout.
set admintimeout { integer }  Administrator timeout for this access profile (0 - 480 min, default = 10, 0 means never timeout). range[1-480]
next
end
```

system admin

Use this command to add, edit, and delete administrator accounts.

```
config system admin
  edit { name }
  # Configure admin users.
  set name { string } User name. size[35]
  set wildcard { enable | disable } Enable/disable wildcard RADIUS authentication.
  set remote-auth { enable | disable } Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.
  set remote-group { string } User group name used for remote auth. size[35]
  set password { password_string } Admin user password. size[128]
  set peer-auth { enable | disable } Set to enable peer certificate authentication (for HTTPS admin access).
  set peer-group { string } Name of peer group defined under config user peergrp or user group defined under config user group. Used for peer
certificate authentication (for HTTPS admin access). size[35]
  set trusthost1 { ipv4 classnet } 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.
  set trusthost2 { ipv4 classnet } 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.
  set trusthost3 { ipv4 classnet } 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.
  set trusthost4 { ipv4 classnet } 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.
  set trusthost5 { ipv4 classnet } 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.
  set trusthost6 { ipv4 classnet } 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.
  set trusthost7 { ipv4 classnet } 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.
  set trusthost8 { ipv4 classnet } 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.
  set trusthost9 { ipv4 classnet } 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.
  set trusthost10 { ipv4 classnet } 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.
  set ip6-trusthost1 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
  set ip6-trusthost2 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
```

```

        set ip6-trusthost3 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost4 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost5 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost6 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost7 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost8 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost9 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set ip6-trusthost10 { ipv6 prefix } Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access
from any IPv6 address.
        set accprofile { string } Access profile for this administrator. Access profiles control administrator access to FortiGate features. size
[35] - datasource(s): system.accprofile.name
        set allow-remove-admin-session { enable | disable } Enable/disable allow admin session to be removed by privileged admin users.
        set comments { string } Comment. size[255]
        set hidden { integer } Admin user hidden attribute. range[0-255]
    config vdom
        edit { name }
            # Virtual domain(s) that the administrator can access.
            set name { string } Virtual domain name. size[64] - datasource(s): system.vdom.name
        next
        set ssh-public-key1 { string } Public key of an SSH client. The client is authenticated without being asked for credentials. Create the pub-
lic-private key pair in the SSH client application.
        set ssh-public-key2 { string } Public key of an SSH client. The client is authenticated without being asked for credentials. Create the pub-
lic-private key pair in the SSH client application.
        set ssh-public-key3 { string } Public key of an SSH client. The client is authenticated without being asked for credentials. Create the pub-
lic-private key pair in the SSH client application.
        set ssh-certificate { string } Select the certificate to be used by the FortiGate for authentication with an SSH client. size[35] - data-
source(s): certificate.local.name
        set schedule { string } Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions. size[35]
        set accprofile-override { enable | disable } 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.
        set radius-vdom-override { enable | disable } Enable to use the names of VDOMs provided by the remote authentication server to control the
VDOMs that this administrator can access.
        set password-expire { string } Password expire time.
        set force-password-change { enable | disable } Enable/disable force password change on next login.
    config gui-dashboard
        edit { id }

```

```
# GUI dashboards.
set id { integer }   Dashboard ID. range[0-4294967295]
set name { string }  Dashboard name. size[35]
set scope { global | vdom }  Dashboard scope.
    global Global.
    vdom VDOM.
set layout-type { responsive | fixed }  Layout type.
    responsive Responsive.
    fixed Fixed grid.
set columns { integer }  Number of columns. range[5-20]
config widget
edit { id }
    # Dashboard widgets.
    set id { integer }  Widget ID. range[0-4294967295]
    set type { option }  Widget type.
        sysinfo          System Information.
        licinfo          License Information.
        forticloud       FortiCloud Licenses.
        cpu-usage        CPU Usage.
        memory-usage     Memory Usage.
        disk-usage       Disk Usage.
        log-rate         Session Rate.
        sessions         Sessions.
        session-rate     Session Rate.
        tr-history       Traffic History.
        analytics        FortiGuard Analytics.
        usb-modem        USB Modem.
        admins           Administrators.
        security-fabric  Security Fabric.
        security-audit   Security Fabric Audit.
        sensor-info      Sensor Information.
        ha-status        HA Status.
        vulnerability-summary  Vulnerability Summary.
        host-scan-summary  Host Scan Summary.
        fortiview        FortiView.
    set x-pos { integer }  X position. range[0-1000]
    set y-pos { integer }  Y position. range[0-1000]
    set width { integer }  Width. range[1-50]
    set height { integer }  Height. range[1-50]
    set interface { string }  Interface to monitor. size[15] - datasource(s): system.interface.name
    set report-by { option }  Field to aggregate the data by.
        source           Sources.
        destination      Destinations.
```

```

country          Country.
intfpair         Interface pairs.
srcintf         Source interface.
dstintf         Destination interface.
policy          Policy.
wificlient      WiFi clients.
shaper          Shaper.
endpoint-vulnerability Endpoint vulnerability.
endpoint-device  Endpoint device.
application     Application.
cloud-app       Cloud application.
cloud-user      Cloud user.
web-domain      Web domain.
web-category    Web category.
web-search-phrase Search phrase.
threat          Threat.
system          System.
unauth          Failed authentication.
admin           Admin.
vpn            VPN.

set timeframe { option }  Timeframe period of reported data.
    realtime Realtime.
    5min      Last 5 minutes.
    hour      Last hour.
    day       Last 24 hours.
    week      Last week.

set sort-by { string }  Field to sort the data by. size[127]
set visualization { table | bubble | country | chord }  Visualization to use.
    table     Table.
    bubble    Bubble.
    country   Country.
    chord     Chord.

config filters
edit { id }
# FortiView filters.
    set id { integer }  FortiView Filter ID. range[0-4294967295]
    set key { string }  Filter key. size[127]
    set value { string }  Filter value. size[127]
next
next
set two-factor { disable | fortitoken | email | sms }  Enable/disable two-factor authentication.
    disable      Disable two-factor authentication.

```

```

        fortitoken Use FortiToken or FortiToken mobile two-factor authentication.
        email      Send a two-factor authentication code to the configured email-to email address.
        sms        Send a two-factor authentication code to the configured sms-server and sms-phone.
set fortitoken { string } This administrator's FortiToken serial number. size[16]
set email-to { string } This administrator's email address. size[63]
set sms-server { fortiguard | custom } Send SMS messages using the FortiGuard SMS server or a custom server.
        fortiguard Send SMS by FortiGuard.
        custom     Send SMS by custom server.
set sms-custom-server { string } Custom SMS server to send SMS messages to. size[35] - datasource(s): system.sms-server.name
set sms-phone { string } Phone number on which the administrator receives SMS messages. size[15]
set guest-auth { disable | enable } Enable/disable guest authentication.
config guest-usergroups
    edit { name }
        # Select guest user groups.
        set name { string } Select guest user groups. size[64]
    next
set guest-lang { string } Guest management portal language. size[35] - datasource(s): system.custom-language.name
set history0 { password_string } history0 size[128]
set history1 { password_string } history1 size[128]
config login-time
    edit { usr-name }
        # Record user login time.
        set usr-name { string } User name. size[35]
        set last-login { datetime } Last successful login time.
        set last-failed-login { datetime } Last failed login time.
    next
config gui-global-menu-favorites
    edit { id }
        # Favorite GUI menu IDs for the global VDOM.
        set id { string } Select menu ID. size[64]
    next
config gui-vdom-menu-favorites
    edit { id }
        # Favorite GUI menu IDs for VDOMs.
        set id { string } Select menu ID. size[64]
    next
next
end

```

remote-auth {enable | disable}

Enable or disable authentication of this administrator using a remote RADIUS, LDAP, or TACACS+ server. Disabled by default.

wildcard {enable | disable}

Enable or disable wildcard RADIUS authentication. Disabled by default. This option only appears when `remote-auth` is enabled.

remote-group <name>

Group name used for remote authentication. This option only appears when `remote-auth` is enabled.

password <string>

Set the password for the administrator account.

peer-auth {enable | disable}

Enable or disable peer authentication. Disabled by default.

peer-group <name>

Group name for peer authentication. This option only appears when `peer-auth` is enabled.

{trusthost1 ... trusthost10} <ip_address>

Set up to ten IPv4 addresses as trusted IPs for authentication.

{ip6-trusthost1 ... ip6-trusthost10} <ip_address>

Set up to ten IPv6 addresses as trusted IPs for authentication.

accprofile <profile-name>

Set the access profile (also known as admin profile) for the account. Access profiles control administrator access to FortiGate features. Two default profiles are available: `prof_admin` and `super_admin`.

accprofile-override {enable | disable}

Enable or disable allowing the remote server to override the administrator's access profile. Disabled by default. This option only appears when `remote-auth` is enabled.

radius-vdom-override {enable | disable}

Enable or disable allowing the remote server to override VDOM access. Only available with wildcard RADIUS authentication. Disabled by default. This option only appears when `remote-auth` is enabled.

allow-remove-admin-session {enable | disable}

Enable or disable allowing session initiated by this administrator to be removed by a privileged administrator. Enabled by default. This field is available for accounts with the `super_admin` profile.

comments <string>

Add comments.

vdom <vdom-name>

Select the virtual domain(s) that the administrator can access.

{ssh-public-key1 | ssh-public-key2 | ssh-public-key3} <key-type> <key-value>

Set up to three SSH public keys.

ssh-certificate <certificate-name>

Set a certificate for PKI authentication of the administrator.

schedule <schedule-name>

Set a schedule for the account.

password-expire

Enter the date and time that this administrator's password expires. Enter zero values for no expiry (this is set by default). Date format is YYYY-MM-DD. Time format is HH:MM:SS. This is available only if `config system password-policy` is enabled.

force-password-change {enable | disable}

Enable or disable requiring this administrator to change password at next login. Disabled by default. Disabling this option does not prevent required password changes due to password policy violation or expiry. This is available only if `config system password-policy` is enabled.

two-factor {enable | disable}

Enable or disable two-factor authentication. Disabled by default.

email-to <email-address>

Set an email address to use for two-factor authentication.

sms-server <server>

Set provider to use to send SMS messages for two-factor authentication. This list of available providers is configured using `config system sms-server`.

sms-phone <phone-number>

Set a phone number to use for two-factor authentication.

guest-auth {enable | disable}

Enable to restrict the admin account to guest account provisioning. Disabled by default.

guest-usergroups <group-name>

Set the user group(s) to be used for guest user accounts created by this administrator account. This option only appears when the account is restricted to guest account provisioning.

guest-lang <language>

Select a language to use for the guest management portal.

system alarm

Introduction.

```
config system alarm
  set status { enable | disable }  Enable/disable alarm.
  set audible { enable | disable }  Enable/disable audible alarm.
config groups
  edit { id }
  # Alarm groups.
  set id { integer }  Group ID. range[0-4294967295]
  set period { integer }  Time period in seconds (0 = from start up). range[0-4294967295]
  set admin-auth-failure-threshold { integer }  Admin authentication failure threshold. range[0-1024]
  set admin-auth-lockout-threshold { integer }  Admin authentication lockout threshold. range[0-1024]
  set user-auth-failure-threshold { integer }  User authentication failure threshold. range[0-1024]
  set user-auth-lockout-threshold { integer }  User authentication lockout threshold. range[0-1024]
  set replay-attempt-threshold { integer }  Replay attempt threshold. range[0-1024]
  set self-test-failure-threshold { integer }  Self-test failure threshold. range[0-1]
  set log-full-warning-threshold { integer }  Log full warning threshold. range[0-1024]
  set encryption-failure-threshold { integer }  Encryption failure threshold. range[0-1024]
  set decryption-failure-threshold { integer }  Decryption failure threshold. range[0-1024]
config fw-policy-violations
  edit { id }
  # Firewall policy violations.
  set id { integer }  Firewall policy violations ID. range[0-4294967295]
  set threshold { integer }  Firewall policy violation threshold. range[0-1024]
  set src-ip { ipv4 address }  Source IP (0=all).
  set dst-ip { ipv4 address }  Destination IP (0=all).
  set src-port { integer }  Source port (0=all). range[0-65535]
  set dst-port { integer }  Destination port (0=all). range[0-65535]
  next
  set fw-policy-id { integer }  Firewall policy ID. range[0-4294967295]
  set fw-policy-id-threshold { integer }  Firewall policy ID threshold. range[0-1024]
next
end
```

system alias

Introduction.

```
config system alias
  edit { name }
  # Configure alias command.
  set name { string }  Alias command name. size[35]
  set command { string }  Command list to execute. size[255]
next
end
```

system api-user

Introduction.

```
config system api-user
  edit { name }
  # Configure API users.
  set name { string }   User name. size[35]
  set comments { string } Comment. size[255]
  set api-key { password_string } Admin user password. size[128]
  set accprofile { string } Admin user access profile. size[35] - datasource(s): system.accprofile.name
  config vdom
    edit { name }
    # Virtual domains.
    set name { string } Virtual domain name. size[64] - datasource(s): system.vdom.name
    next
  set schedule { string } Schedule name. size[35]
  set cors-allow-origin { string } Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible. size[269]
  set peer-auth { enable | disable } Enable/disable peer authentication.
  set peer-group { string } Peer group name. size[35]
  config trusthost
    edit { id }
    # Trusthost.
    set id { integer } Table ID. range[0-4294967295]
    set type { ipv4-trusthost | ipv6-trusthost } Trusthost type.
      ipv4-trusthost IPv4 trusthost.
      ipv6-trusthost IPv6 trusthost.
    set ipv4-trusthost { ipv4 classnet } IPv4 trusted host address.
    set ipv6-trusthost { ipv6 prefix } IPv6 trusted host address.
    next
  next
end
```

system arp-table

Introduction.

```
config system arp-table
  edit { id }
  # Configure ARP table.
  set id { integer } Unique integer ID of the entry. range[0-4294967295]
  set interface { string } Interface name. size[15] - datasource(s): system.interface.name
  set ip { ipv4 address } IP address.
  set mac { mac address } MAC address.
  next
end
```

system auto-install

Introduction.

```
config system auto-install
  set auto-install-config { enable | disable }  Enable/disable auto install the config in USB disk.
  set auto-install-image { enable | disable }  Enable/disable auto install the image in USB disk.
  set default-config-file { string }  Default config file name in USB disk. size[127]
  set default-image-file { string }  Default image file name in USB disk. size[127]
end
```


system auto-script

Introduction.

```
config system auto-script
  edit { name }
  # Configure auto script.
  set name { string }  Auto script name. size[35]
  set interval { integer }  Repeat interval in seconds. range[0-31557600]
  set repeat { integer }  Number of times to repeat this script (0 = infinite). range[0-65535]
  set start { manual | auto }  Script starting mode.
    manual Starting manually.
    auto Starting automatically.
  set script { string }  List of FortiOS CLI commands to repeat. size[255]
  set output-size { integer }  Number of megabytes to limit script output to (10 - 1024, default = 10). range[10-1024]
next
end
```

system autoupdate push-update

Introduction.

```
config system autoupdate push-update
  set status { enable | disable }  Enable/disable push updates.
  set override { enable | disable }  Enable/disable push update override server.
  set address { ipv4 address any }  Push update override server.
  set port { integer }  Push update override port. (Do not overlap with other service ports) range[0-65535]
end
```

system autoupdate schedule

Introduction.

```
config system autoupdate schedule
  set status { enable | disable }  Enable/disable scheduled updates.
  set frequency { every | daily | weekly }  Update frequency.
    every  Time interval.
    daily  Every day.
    weekly Every week.
  set time { string }  Update time.
  set day { option }  Update day.
    Sunday  Update every Sunday.
    Monday  Update every Monday.
    Tuesday  Update every Tuesday.
    Wednesday  Update every Wednesday.
    Thursday  Update every Thursday.
    Friday  Update every Friday.
    Saturday  Update every Saturday.
end
```

system autoupdate tunneling

Introduction.

```
config system autoupdate tunneling
  set status { enable | disable }  Enable/disable web proxy tunnelling.
  set address { string }  Web proxy IP address or FQDN. size[63]
  set port { integer }  Web proxy port. range[0-65535]
  set username { string }  Web proxy username. size[49]
  set password { password_string }  Web proxy password. size[128]
end
```

system central-management

Use this command to configure central management for your FortiGate unit. Central management uses a remote location to backup, restore, and monitor the FortiGate unit's configuration. This can be either a FortiManager or the FortiCloud network.

```
config system central-management
  set mode { normal | backup } Central management mode.
    normal Manage and configure this FortiGate from FortiManager.
    backup Manage and configure this FortiGate locally and back up its configuration to FortiManager.
  set type { fortimanager | fortiguard | none } Central management type.
    fortimanager FortiManager.
    fortiguard Central management of this FortiGate using FortiCloud.
    none No central management.
  set schedule-config-restore { enable | disable } Enable/disable allowing the central management server to restore the configuration of this FortiGate.
  set schedule-script-restore { enable | disable } Enable/disable allowing the central management server to restore the scripts stored on this FortiGate.
  set allow-push-configuration { enable | disable } Enable/disable allowing the central management server to push configuration changes to this FortiGate.
  set allow-pushd-firmware { enable | disable } Enable/disable allowing the central management server to push firmware updates to this FortiGate.
  set allow-remote-firmware-upgrade { enable | disable } Enable/disable remotely upgrading the firmware on this FortiGate from the central management server.
  set allow-monitor { enable | disable } Enable/disable allowing the central management server to remotely monitor this FortiGate
  set serial-number { string } Serial number.
  set fmg { string } IP address or FQDN of the FortiManager.
  set fmg-source-ip { ipv4 address } IPv4 source address that this FortiGate uses when communicating with FortiManager.
  set fmg-source-ip6 { ipv6 address } IPv6 source address that this FortiGate uses when communicating with FortiManager.
  set vdom { string } Virtual domain (VDOM) name to use when communicating with FortiManager. size[31] - datasource(s): system.vdom.name
config server-list
  edit { id }
    # Additional servers that the FortiGate can use for updates (for AV, IPS, updates) and ratings (for web filter and antispam ratings) servers.
    set id { integer } ID. range[0-4294967295]
    set server-type { update | rating } FortiGuard service type.
      update AV, IPS, and AV-query update server.
      rating Web filter and anti-spam rating server.
    set addr-type { ipv4 | ipv6 | fqdn } Indicate whether the FortiGate communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.
      ipv4 IPv4 address.
      ipv6 IPv6 address.
```

```
        fqdn FQDN.
    set server-address { ipv4 address } IPv4 address of override server.
    set server-address6 { ipv6 address } IPv6 address of override server.
    set fqdn { string } FQDN address of override server. size[255]
next
set include-default-servers { enable | disable } Enable/disable inclusion of public FortiGuard servers in the override server list.
set enc-algorithm { default | high | low } Encryption strength for communications between the FortiGate and central management.
    default High strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD.
    high 128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-
RSA-AES128-SHA, AES128-SHA.
    low 64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CBC-SHA, DES-CBC-SHA, DES-CBC-MD5.
end
```

mode {normal | backup}

Identify central management mode. Default is normal.

- **normal**: manage and configure the connected FortiGate devices from the FortiManager GUI.
- **backup**: backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally.

type {fortiguard | fortimanager | none}

Specify the type of central management. Setting `type` to `fortiguard` in the CLI is the same as setting it to FortiCloud in the GUI. FortiCloud used to be known as the FortiGuard Analysis and Management Service network. Default is `fortimanager`.

schedule-config-restore {enable | disable}

Enable/disable scheduling the restoration of your FortiGate's configuration. Default is enable.

schedule-script-restore {enable | disable}

Enable/disable scheduling the restoration of your FortiGate's configuration through scripts. Default is enable.

allow-push-configuration {enable | disable}

Enable/disable configuration image push updates for your FortiGate. Default is enable.

allow-pushd-firmware {enable | disable}

Enable/disable push firmware. Default is enable.

allow-remote-firmware-upgrade {enable | disable}

Enable/disable remote upgrading of your FortiGate to a new firmware. Default is enable.

allow-monitor {enable | disable}

Enable/disable remote monitoring of your FortiGate unit. Default is enable.

fmg <fmg_ipv4>

Specify the IP address or FQDN of the remote FortiManager server. Appears only when `type` is set to `fortimanager`.

fmg-source-ip <address_ipv4>

Specify the source IPv4 address to use when connecting to FortiManager. Appears only when `type` is set to `fortimanager`.

fmg-source-ip6

Specify the source IPv6 address to use when connecting to FortiManager. Appears only when `type` is set to `fortimanager`.

vdom <name_str>

Optional. Specify name of virtual domain (VDOM) to use when communicating with FortiManager. Default is root.

enc-algorithm {default | high | low}

Specify encryption strength for communications between the FortiGate unit and FortiManager. Default is high.

- `default`: high- and medium-strength algorithms
- `high`: 128-bit and larger key length algorithms
- `low`: 64-bit or 56-bit key length algorithms without export restrictions

config server-list**server-type {rating | update}**

Specify the FortiGuard service type.

- `rating`: web filter or anti-spam rating server
- `update`: AV, IPS, or AV-query server

`addr-type {ipv4 | ipv6}`

Identify override server's address type.

`server-address <ipv4>`

Specify the override server's IPv4 address.

`server-address6 <ipv6>`

Specify the override server's IPv6 address.

system cluster-sync

Introduction.

```
config system cluster-sync
  edit { sync-id }
    # Configure FortiGate Session Life Support Protocol (FGSP) session synchronization.
    set sync-id { integer } Sync ID. range[0-255]
    set peervd { string } VDOM that contains the session synchronization link interface on the peer unit. Usually both peers would have the
same peervd. size[31] - datasource(s): system.vdom.name
    set peerip { ipv4 address } IP address of the interface on the peer unit that is used for the session synchronization link.
  config syncvd
    edit { name }
      # Sessions from these VDOMs are synchronized using this session synchronization configuration.
      set name { string } VDOM name. size[64] - datasource(s): system.vdom.name
    next
  config down-intfs-before-sess-sync
    edit { name }
      # List of interfaces to be turned down before session synchronization is complete.
      set name { string } Interface name. size[64] - datasource(s): system.interface.name
    next
  set hb-interval { integer } Heartbeat interval (1 - 10 sec). range[1-10]
  set hb-lost-threshold { integer } Lost heartbeat threshold (1 - 10). range[1-10]
  set slave-add-ike-routes { enable | disable } Enable/disable IKE route announcement on the backup unit.
  set srcintf { string } Only sessions from this interface are synchronized. You can only enter one interface name. To synchronize ses-
sions for multiple source interfaces, add multiple filters. size[15] - datasource(s): system.interface.name
  set dstintf { string } Only sessions to this interface are synchronized. You can only enter one interface name. To synchronize sessions
to multiple destination interfaces, add multiple filters. size[15] - datasource(s): system.interface.name
  set srcaddr { ipv4 classnet any } Only sessions from this IPv4 address are synchronized. You can only enter one address. To synchronize
sessions from multiple source addresses, add multiple filters.
  set dstaddr { ipv4 classnet any } Only sessions to this IPv4 address are synchronized. You can only enter one address. To synchronize
sessions for multiple destination addresses, add multiple filters.
  set srcaddr6 { ipv6 network } Only sessions from this IPv6 address are synchronized. You can only enter one address. To synchronize ses-
sions from multiple source addresses, add multiple filters.
  set dstaddr6 { ipv6 network } Only sessions to this IPv6 address are synchronized. You can only enter one address. To synchronize ses-
sions for multiple destination addresses, add multiple filters.
  config custom-service
    edit { id }
      # Only sessions using these custom services are synchronized. Use source and destination port ranges to define these custome
```

```
services.  
    set id { integer }    Custom service ID. range[0-4294967295]  
    set src-port-range { string }    Custom service source port range.  
    set dst-port-range { string }    Custom service destination port range.  
next  
next  
end
```

system console

Introduction.

```
config system console
  set mode { batch | line }  Console mode.
    batch  Batch mode.
    line   Line mode.
  set baudrate { option }  Console baud rate.
    9600   9600
    19200  19200
    38400  38400
    57600  57600
    115200 115200
  set output { standard | more }  Console output mode.
    standard  Standard output.
    more      More page output.
  set login { enable | disable }  Enable/disable serial console and FortiExplorer.
  set fortieplorer { enable | disable }  Enable/disable access for FortiExplorer.
end
```

system csf

Configure the network as a Cooperative Security Fabric (CSF).

```
config system csf
  set status { enable | disable }  Enable/disable Security Fabric.
  set upstream-ip { ipv4 address }  The IP address of the FortiGate upstream from this FortiGate in the Security Fabric.
  set upstream-port { integer }    The port number to use to communicate with the FortiGate upstream from this FortiGate in the Security Fabric
  (default = 8013). range[1-65535]
  set group-name { string }        Security Fabric group name. All FortiGates in a Security Fabric must have the same group name. size[35]
  set group-password { password_string } Security Fabric group password. All FortiGates in a Security Fabric must have the same group password.
  size[128]
  set logging-mode { default | local } Logging mode (the root FortiGate in a Security Fabric must send logs to FortiAnalyzer).
    default This FortiGate logs traffic if it is not logged by another FortiGate in the Security Fabric.
    local   This FortiGate logs traffic according to its local logging configuration.
  set management-ip { ipv4 address } Management IP address of this FortiGate. Used to log into this FortiGate from another FortiGate in the Secur-
  ity Fabric.
end
```

status {enable | disable}

Enable or disable the security fabric. The default is `disable`.

upstream-ip <ip-address>

The IP address of the upstream FortiGate.

upstream-port <port-number>

The port used by the upstream FortiGate for communication within the security fabric. The default is `8013`.

group-name <name>

The name of the security fabric.

group-password <password>

The password for the security fabric.

logging mode {default | local}

The location of logs for the fabric. The two options are:

- `default`: Traffic is logged if it has not already been logged by another FortiGate
- `local`: All traffic logging is done according to the FortiGate's local settings

The default is `default`.

management-ip <ip-address>

The management IP address of this FortiGate.

system custom-language

Introduction.

```
config system custom-language
  edit { name }
  # Configure custom languages.
  set name { string } Name. size[35]
  set filename { string } Custom language file path. size[63]
  set comments { string } Comment. size[255]
next
end
```

system ddns

Introduction.

```
config system ddns
  edit { ddnsid }
  # Configure DDNS.
  set ddnsid { integer }   DDNS ID. range[0-4294967295]
  set ddns-server { option }  Select a DDNS service provider.
    dyndns.org      members.dyndns.org and dnsalias.com
    dyns.net        www.dyns.net
    tzo.com         rh.tzo.com
    vavic.com       Peanut Hull
    dipdns.net      dipdnsserver.dipdns.com
    now.net.cn     ip.todayisp.com
    dhs.org         members.dhs.org
    easydns.com    members.easydns.com
    genericDDNS    Generic DDNS based on RFC2136.
    FortiGuardDDNS FortiGuard DDNS service.
    noip.com       dynupdate.no-ip.com
  set ddns-server-ip { ipv4 address }  Generic DDNS server IP.
  set ddns-zone { string }  Zone of your domain name (for example, DDNS.com). size[64]
  set ddns-ttl { integer }  Time-to-live for DDNS packets. range[60-86400]
  set ddns-auth { disable | tsig }  Enable/disable TSIG authentication for your DDNS server.
    disable  Disable DDNS authentication.
    tsig     Enable TSIG authentication based on RFC2845.
  set ddns-keyname { string }  DDNS update key name. size[64]
  set ddns-key { string }  DDNS update key (base 64 encoding).
  set ddns-domain { string }  Your fully qualified domain name (for example, yourname.DDNS.com). size[64]
  set ddns-username { string }  DDNS user name. size[64]
  set ddns-sn { string }  DDNS Serial Number. size[64]
  set ddns-password { password_string }  DDNS password. size[128]
  set use-public-ip { disable | enable }  Enable/disable use of public IP address.
  set update-interval { integer }  DDNS update interval (60 - 2592000 sec, default = 300). range[60-2592000]
  set clear-text { disable | enable }  Enable/disable use of clear text connections.
  set ssl-certificate { string }  Name of local certificate for SSL connections. size[35] - datasource(s): certificate.local.name
  set bound-ip { ipv4 address }  Bound IP address.
config monitor-interface
  edit { interface-name }
```

```
        # Monitored interface.
        set interface-name { string } Interface name. size[64] - datasource(s): system.interface.name
    next
end
```


system dedicated-mgmt

Introduction.

```
config system dedicated-mgmt
  set status { enable | disable }  Enable/disable dedicated management.
  set interface { string }  Dedicated management interface. size[15] - datasource(s): system.interface.name
  set default-gateway { ipv4 address }  Default gateway for dedicated management interface.
  set dhcp-server { enable | disable }  Enable/disable DHCP server on management interface.
  set dhcp-netmask { ipv4 netmask }  DHCP netmask.
  set dhcp-start-ip { ipv4 address }  DHCP start IP for dedicated management.
  set dhcp-end-ip { ipv4 address }  DHCP end IP for dedicated management.
end
```

system {dhcp server | dhcp6 server}

Configure DHCP servers used to assign IP settings, including IP addresses, to devices connected to a FortiGate interface.

```
config system dhcp server
  edit { id }
  # Configure DHCP servers.
  set id { integer } ID. range[0-4294967295]
  set status { disable | enable } Enable/disable this DHCP configuration.
  set lease-time { integer } Lease time in seconds, 0 means unlimited. range[300-8640000]
  set mac-acl-default-action { assign | block } MAC access control default action (allow or block assigning IP settings).
    assign Allow the DHCP server to assign IP settings to clients on the MAC access control list.
    block Block the DHCP server from assigning IP settings to clients on the MAC access control list.
  set forticlient-on-net-status { disable | enable } Enable or disable FortiClient-On-Net service for this DHCP server.
  set dns-service { local | default | specify } Options for assigning DNS servers to DHCP clients.
    local IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.
    default Clients are assigned the FortiGate's configured DNS servers.
    specify Specify up to 3 DNS servers in the DHCP server configuration.
  set dns-server1 { ipv4 address } DNS server 1.
  set dns-server2 { ipv4 address } DNS server 2.
  set dns-server3 { ipv4 address } DNS server 3.
  set wifi-acl { ipv4 address } WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).
  set wifi-ac2 { ipv4 address } WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).
  set wifi-ac3 { ipv4 address } WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).
  set ntp-service { local | default | specify } Options for assigning Network Time Protocol (NTP) servers to DHCP clients.
    local IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.
    default Clients are assigned the FortiGate's configured NTP servers.
    specify Specify up to 3 NTP servers in the DHCP server configuration.
  set ntp-server1 { ipv4 address } NTP server 1.
  set ntp-server2 { ipv4 address } NTP server 2.
  set ntp-server3 { ipv4 address } NTP server 3.
  set domain { string } Domain name suffix for the IP addresses that the DHCP server assigns to clients. size[35]
  set wins-server1 { ipv4 address } WINS server 1.
  set wins-server2 { ipv4 address } WINS server 2.
  set default-gateway { ipv4 address } Default gateway IP address assigned by the DHCP server.
  set next-server { ipv4 address } IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.
  set netmask { ipv4 netmask } Netmask assigned by the DHCP server.
  set interface { string } DHCP server can assign IP configurations to clients connected to this interface. size[15] - datasource(s): sys-
  tem.interface.name
```

```
config ip-range
  edit { id }
  # DHCP IP range configuration.
  set id { integer } ID. range[0-4294967295]
  set start-ip { ipv4 address } Start of IP range.
  set end-ip { ipv4 address } End of IP range.
  next
set timezone-option { disable | default | specify } Options for the DHCP server to set the client's time zone.
  disable Do not set the client's time zone.
  default Clients are assigned the FortiGate's configured time zone.
  specify Specify the time zone to be assigned to DHCP clients.
set timezone { option } Select the time zone to be assigned to DHCP clients.
  01 (GMT-11:00) Midway Island, Samoa
  02 (GMT-10:00) Hawaii
  03 (GMT-9:00) Alaska
  04 (GMT-8:00) Pacific Time (US & Canada)
  05 (GMT-7:00) Arizona
  81 (GMT-7:00) Baja California Sur, Chihuahua
  06 (GMT-7:00) Mountain Time (US & Canada)
  07 (GMT-6:00) Central America
  08 (GMT-6:00) Central Time (US & Canada)
  09 (GMT-6:00) Mexico City
  10 (GMT-6:00) Saskatchewan
  11 (GMT-5:00) Bogota, Lima, Quito
  12 (GMT-5:00) Eastern Time (US & Canada)
  13 (GMT-5:00) Indiana (East)
  74 (GMT-4:00) Caracas
  14 (GMT-4:00) Atlantic Time (Canada)
  77 (GMT-4:00) Georgetown
  15 (GMT-4:00) La Paz
  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
  87 (GMT-3:00) Paraguay
  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
26 (GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
27 (GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
28 (GMT+1:00) Brussels, Copenhagen, Madrid, Paris
78 (GMT+1:00) Namibia
29 (GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb
30 (GMT+1:00) West Central Africa
31 (GMT+2:00) Athens, Sofia, Vilnius
32 (GMT+2:00) Bucharest
33 (GMT+2:00) Cairo
34 (GMT+2:00) Harare, Pretoria
35 (GMT+2:00) Helsinki, Riga, Tallinn
36 (GMT+2:00) Jerusalem
37 (GMT+3:00) Baghdad
38 (GMT+3:00) Kuwait, Riyadh
83 (GMT+3:00) Moscow
84 (GMT+3:00) Minsk
40 (GMT+3:00) Nairobi
85 (GMT+3:00) Istanbul
41 (GMT+3:30) Tehran
42 (GMT+4:00) Abu Dhabi, Muscat
43 (GMT+4:00) Baku
39 (GMT+3:00) St. Petersburg, Volgograd
44 (GMT+4:30) Kabul
46 (GMT+5:00) Islamabad, Karachi, Tashkent
47 (GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi
51 (GMT+5:30) Sri Jayawardenepara
48 (GMT+5:45) Kathmandu
45 (GMT+5:00) Ekaterinburg
49 (GMT+6:00) Almaty, Novosibirsk
50 (GMT+6:00) Astana, Dhaka
52 (GMT+6:30) Rangoon
53 (GMT+7:00) Bangkok, Hanoi, Jakarta
54 (GMT+7:00) Krasnoyarsk
55 (GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk
56 (GMT+8:00) Ulaan Bataar
57 (GMT+8:00) Kuala Lumpur, Singapore
58 (GMT+8:00) Perth
59 (GMT+8:00) Taipei
60 (GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
62 (GMT+9:30) Adelaide
63 (GMT+9:30) Darwin
61 (GMT+9:00) Yakutsk
```

```

64 (GMT+10:00) Brisbane
65 (GMT+10:00) Canberra, Melbourne, Sydney
66 (GMT+10:00) Guam, Port Moresby
67 (GMT+10:00) Hobart
68 (GMT+10:00) Vladivostok
69 (GMT+10:00) Magadan
70 (GMT+11:00) Solomon Is., New Caledonia
71 (GMT+12:00) Auckland, Wellington
72 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
00 (GMT+12:00) Eniwetok, Kwajalein
82 (GMT+12:45) Chatham Islands
73 (GMT+13:00) Nuku'alofa
86 (GMT+13:00) Samoa
76 (GMT+14:00) Kiritimati
set tftp-server { string } Hostname or IP address of the TFTP server. size[63]
set filename { string } Name of the boot file on the TFTP server. size[127]
config options
edit { id }
# DHCP options.
set id { integer } ID. range[0-4294967295]
set code { integer } DHCP option code. range[0-255]
set type { hex | string | ip } DHCP option type.
    hex DHCP option in hex.
    string DHCP option in string.
    ip DHCP option in IP.
set value { string } DHCP option value. size[312]
set ip { string } DHCP option IPs.
next
set server-type { regular | ipsec } DHCP server can be a normal DHCP server or an IPsec DHCP server.
    regular Regular DHCP service.
    ipsec DHCP over IPsec service.
set ip-mode { range | usrgrp } Method used to assign client IP.
    range Use range defined by start-ip/end-ip to assign client IP.
    usrgrp Use user-group defined method to assign client IP.
set conflicted-ip-timeout { integer } Time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be
reused. range[60-8640000]
set ipsec-lease-hold { integer } DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry). range[0-
8640000]
set auto-configuration { disable | enable } Enable/disable auto configuration.
set ddns-update { disable | enable } Enable/disable DDNS update for DHCP.
set ddns-update-override { disable | enable } Enable/disable DDNS update override for DHCP.
set ddns-server-ip { ipv4 address } DDNS server IP.
set ddns-zone { string } Zone of your domain name (ex. DDNS.com). size[64]

```

```

set ddns-auth { disable | tsig }  DDNS authentication mode.
    disable  Disable DDNS authentication.
    tsig     TSIG based on RFC2845.
set ddns-keyname { string }  DDNS update key name. size[64]
set ddns-key { string }  DDNS update key (base 64 encoding).
set ddns-ttl { integer }  TTL. range[60-86400]
set vci-match { disable | enable }  Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching
VCI are served.
config vci-string
    edit { vci-string }
        # One or more VCI strings in quotes separated by spaces.
        set vci-string { string }  VCI strings. size[255]
    next
config exclude-range
    edit { id }
        # Exclude one or more ranges of IP addresses from being assigned to clients.
        set id { integer }  ID. range[0-4294967295]
        set start-ip { ipv4 address }  Start of IP range.
        set end-ip { ipv4 address }  End of IP range.
    next
config reserved-address
    edit { id }
        # Options for the DHCP server to assign IP settings to specific MAC addresses.
        set id { integer }  ID. range[0-4294967295]
        set ip { ipv4 address }  IP address to be reserved for the MAC address.
        set mac { mac address }  MAC address of the client that will get the reserved IP address.
        set action { assign | block | reserved }  Options for the DHCP server to configure the client with the reserved MAC address.
            assign  Configure the client with this MAC address like any other client.
            block  Block the DHCP server from assigning IP settings to the client with this MAC address.
            reserved  Assign the reserved IP address to the client with this MAC address.
        set description { string }  Description. size[255]
    next
next
end

config system dhcp6 server
    edit { id }
        # Configure DHCPv6 servers.
        set id { integer }  ID. range[0-4294967295]
        set status { disable | enable }  Enable/disable this DHCPv6 configuration.
        set rapid-commit { disable | enable }  Enable/disable allow/disallow rapid commit.
        set lease-time { integer }  Lease time in seconds, 0 means unlimited. range[300-8640000]

```

```

set dns-service { delegated | default | specify } Options for assigning DNS servers to DHCPv6 clients.
    delegated Delegated DNS settings.
    default Clients are assigned the FortiGate's configured DNS servers.
    specify Specify up to 3 DNS servers in the DHCPv6 server configuration.
set dns-search-list { delegated | specify } DNS search list options.
    delegated Delegated the DNS search list.
    specify Specify the DNS search list.
set dns-server1 { ipv6 address } DNS server 1.
set dns-server2 { ipv6 address } DNS server 2.
set dns-server3 { ipv6 address } DNS server 3.
set domain { string } Domain name suffix for the IP addresses that the DHCP server assigns to clients. size[35]
set subnet { ipv6 prefix } Subnet or subnet-id if the IP mode is delegated.
set interface { string } DHCP server can assign IP configurations to clients connected to this interface. size[15] - datasource(s): sys-
tem.interface.name
set option1 { string } Option 1.
set option2 { string } Option 2.
set option3 { string } Option 3.
set upstream-interface { string } Interface name from where delegated information is provided. size[15] - datasource(s): sys-
tem.interface.name
set ip-mode { range | delegated } Method used to assign client IP.
    range Use range defined by start IP/end IP to assign client IP.
    delegated Use delegated prefix method to assign client IP.
config ip-range
    edit { id }
    # DHCP IP range configuration.
    set id { integer } ID. range[0-4294967295]
    set start-ip { ipv6 address } Start of IP range.
    set end-ip { ipv6 address } End of IP range.
next
end

```

status {disable | enable}

Enable or disable this DHCP server, default is enable.

lease-time <integer>

Lease time in seconds, value between 300 and 8640000 (5 minutes to almost 100 days), 0 for unlimited lease time, default is 604800.

mac-acl-default-action {assign | block}

MAC access control default action. Set whether or not the DHCP server assigns network settings to a DHCP client with a MAC address that is on the MAC address control list.

- `assign` allow the DHCP server to assign IP settings to a client on the MAC address control list.
 - `block` block the DHCP from assigning IP settings to a client on the MAC address control list.
-

forticlient-on-net-status {disable | enable}

Enable or disable the FortiClient-On-Net service for this DHCP server, default is enable.

dns-service {local | default | specify}

How the DHCP clients are assigned DNS servers.

- `local` IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.
 - `default` IP addresses of the DNS servers added to the FortiGate configuration become the client's DNS server IP addresses.
 - `specify` specify up to 3 DNS servers in the DHCP server configuration.
-

dns-server1 <ip>

Set the IP address of DNS server(s) which will be used by DHCP clients, up to three DNS servers (dns-server1, dns-server2, and dns-server3).

wifi-ac1 <ip>

Set the IP address of up to three WiFi Access Controller(s) (wifi-ac1, wifi-ac2, and wifi-ac3). For DHCP option 138 to use DHCP to send WiFi access controller IP addresses to Wireless Termination Points (WTPs) ([RFC 5417](#)).

ntp-service {local | default | specify}

How the DHCP clients are assigned Network Time Protocol (NTP) servers.

- `local` IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.
- `default` IP addresses of the NTP servers added to the FortiGate configuration become the client's NTP server IP addresses.
- `specify` specify up to 3 NTP servers in the DHCP server configuration.

ntp-server1 <ip>

Set the IP address of NTP server(s), up to three NTP servers (ntp-server1, ntp-server2, and ntp-server3).

domain <string>

Domain name suffix for the IP addresses that the DHCP server assigns to clients.

wins-server1 <ip>

Set the IP address of WINS server(s), up to two WINS servers (wins-server1, and wins-server2).

default-gateway <ip>

The default gateway IP address that will be used by DHCP clients as their default gateway.

next-server <ip>

The IP address of the next bootstrap server. Add an IP address if you are using a secondary DHCP server to assign IP configuration options.

netmask <netmask>

The netmask assigned by the DHCP server

interface <interface-name>

The DHCP server can assign IP configurations to DHCP clients connected to this interface.

config ip-range

DHCP IP range configuration.

start-ip <ip>

The first IP of the range.

end-ip <ip>

The last IP of the range.

timezone-option {disable | default | specify}

How the DHCP server sets the client's time zone.

- `disable` do not set the client's time zone.
- `default` DHCP clients are assigned the FortiGate's configured time zone.
- `specify` specify the time zone to be assigned to DHCP clients.

timezone <timezone-number>

Select the time zone that the DHCP server assigns to DHCP clients. Available if `timezone-option` is set to `specify`.

tftp-server <string>

Hostname or IP address of the TFTP server.

filename <string>

The file name on the tftp server.

config options

The DHCP options configuration.

code <integer>

The option's code for DHCP, see [RFC 2132](#) for more details.

type {hex | string | ip}

DHCP option in hexadecimal, string, or IP, default is hex.

value <string>

The value is specified as a single octet. Values are available per option, see [RFC 2132](#) for more details.

server-type {regular | ipsec}

Regular DHCP service or DHCP over IPsec services.

conflicted-ip-timeout <integer>

The time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused. Value between 60 to 8640000 seconds (1 minute to 100 days), default is 1800.

auto-configuration {disable | enable}

Disable or enable auto configuration, default is enable.

ddns-update {disable | enable}

Disable or enable Dynamic DNS update for DHCP, default is disable.

vci-match {disable | enable}

Disable or enable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI string are served, default is disabled.

vci-string <strings>

One or more VCI strings in quotes and separated by spaces.

config exclude-range

DHCP exclude range configuration.

start-ip <ip>

The first IP of the excluded range.

end-ip <ip>

The last IP of the excluded range.

config reserved-address

How the DHCP server assigns IP settings to specific MAC addresses.

ip <ip>

The IP address to be reserved for the client with the MAC address. Only valid if `action` is set to `reserved`.

mac <mac-address>

MAC address of the client to be configured by the DHCP server according to the action.

action {assign | block | reserved}

How the DHCP server configures the client with the reserved MAC address.

- `assign` the DHCP server treats the client with this MAC address like any other client.
- `block` block the DHCP server from assigning IP settings to the client with this MAC address.
- `reserved` assign the reserved IP address to the client with this MAC address.

description <string>

Optionally describe the client with this MAC address.

system dns

Configure DNS settings used to resolve domain names to IP addresses, so devices connected to a FortiGate interface can use it.

```
config system dns
  set primary { ipv4 address } Primary DNS server IP address, default is FortiGuard server at 208.81.112.53.
  set secondary { ipv4 address } Secondary DNS server IP address, default is FortiGuard server at 208.81.112.52.
  set domain { string } Domain name suffix for the IP addresses of the DNS server. size[127]
  set ip6-primary { ipv6 address } Primary DNS server IPv6 address.
  set ip6-secondary { ipv6 address } Secondary DNS server IPv6 address.
  set dns-cache-limit { integer } Maximum number of records in the DNS cache. range[0-4294967295]
  set dns-cache-ttl { integer } Duration in seconds that the DNS cache retains information. range[60-86400]
  set cache-notfound-responses { disable | enable } Enable/disable response from the DNS server when a record is not in cache.
  set source-ip { ipv4 address } IP address used by the DNS server as its source IP.
end
```

primary <ip>

The primary DNS server IP address, default is 208.91.112.53, a FortiGuard server.

secondary <ip>

The secondary DNS server IP address, default is 208.91.112.52, a FortiGuard server.

domain <string>

The domain name suffix for the IP addresses of the DNS server.

ip6-primary <ipv6>

The primary DNS server IPv6 address.

ip6-secondary <ipv6>

The secondary DNS server IPv6 address.

dns-cache-limit <integer>

The number of records in the DNS cache, value between 0 and 4294967295, default is 5000.

dns-cache-ttl <integer>

The duration, in seconds, that the DNS cache retains information, value between 60 and 86400, default is 1800.

cache-notfound-responses {disable | enable}

Disable or enable response from the DNS server when a record is not in cache, default is `disable`.

source-ip <ip>

The IP address used by DNS server as it's source IP.

system dns-database

Introduction.

```
config system dns-database
  edit { name }
  # Configure DNS databases.
  set name { string } Zone name. size[35]
  set status { enable | disable } Enable/disable this DNS zone.
  set domain { string } Domain name. size[255]
  set allow-transfer { string } DNS zone transfer IP address list.
  set type { master | slave } Zone type (master to manage entries directly, slave to import entries from other zones).
    master Master DNS zone, to manage entries directly.
    slave Slave DNS zone to import entries from ther DNS zones.
  set view { shadow | public } Zone view (public to serve public clients, shadow to serve internal clients).
    shadow Shadow DNS zone to serve internal clients.
    public Public DNS zone to serve public clients.
  set ip-master { ipv4 address any } IP address of master DNS server. Entries in this master DNS server and imported into the DNS zone.
  set primary-name { string } Domain name of the default DNS server for this zone. size[255]
  set contact { string } 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. size[255]
  set ttl { integer } Default time-to-live value for the entries of this DNS zone (0 - 2147483647 sec, default = 86400). range[0-2147483647]
  set authoritative { enable | disable } Enable/disable authoritative zone.
  set forwarder { string } DNS zone forwarder IP address list.
  set source-ip { ipv4 address } Source IP for forwarding to DNS server.
config dns-entry
  edit { id }
  # DNS entry.
  set id { integer } DNS entry ID. range[0-4294967295]
  set status { enable | disable } Enable/disable resource record status.
  set type { option } Resource record type.
    A Host type.
    NS Name server type.
    CNAME Canonical name type.
    MX Mail exchange type.
    AAAA IPv6 host type.
    PTR Pointer type.
    PTR_V6 IPv6 pointer type.
```

```
set ttl { integer }    Time-to-live for this entry (0 to 2147483647 sec, default = 0). range[0-2147483647]
set preference { integer }    DNS entry preference, 0 is the highest preference (0 - 65535, default = 10) range[0-65535]
set ip { ipv4 address any }    IPv4 address of the host.
set ipv6 { ipv6 address }    IPv6 address of the host.
set hostname { string }    Name of the host. size[255]
set canonical-name { string }    Canonical name of the host. size[255]
next
next
end
```

system dns-server

Introduction.

```
config system dns-server
  edit { name }
  # Configure DNS servers.
  set name { string }  DNS server name. size[15] - datasource(s): system.interface.name
  set mode { recursive | non-recursive | forward-only }  DNS server mode.
    recursive      Shadow DNS database and forward.
    non-recursive  Public DNS database only.
    forward-only   Forward only.
  set dnsfilter-profile { string }  DNS filter profile. size[35] - datasource(s): dnsfilter.profile.name
  next
end
```

system dscp-based-priority

Introduction.

```
config system dscp-based-priority
  edit { id }
  # Configure DSCP based priority table.
  set id { integer }   Item ID. range[0-4294967295]
  set ds { integer }   DSCP(DiffServ) DS value (0 - 63). range[0-63]
  set priority { low | medium | high }   DSCP based priority level.
    low   Low priority.
    medium Medium priority.
    high  High priority.
  next
end
```

system email-server

Introduction.

```
config system email-server
  set type { custom }    Use FortiGuard Message service or custom email server.
                        custom Use custom email server.
  set reply-to { string }  Reply-To email address. size[63]
  set server { string }   SMTP server IP address or hostname. size[63]
  set port { integer }   SMTP server port. range[1-65535]
  set source-ip { ipv4 address } SMTP server IPv4 source IP.
  set source-ip6 { ipv6 address } SMTP server IPv6 source IP.
  set authenticate { enable | disable } Enable/disable authentication.
  set validate-server { enable | disable } Enable/disable validation of server certificate.
  set username { string } SMTP server user name for authentication. size[35]
  set password { password_string } SMTP server user password for authentication. size[128]
  set security { none | starttls | smtps } Connection security used by the email server.
      none      None.
      starttls  STARTTLS.
      smtps     SSL/TLS.
end
```

system fips-cc

Introduction.

```
config system fips-cc
  set status { enable | disable }  Enable/disable FIPS-CC mode.
  set entropy-token { enable | disable | dynamic }  Enable/disable/dynamic entropy token.
  set self-test-period { integer }  Self test period. range[1-1440]
  set key-generation-self-test { enable | disable }  Enable/disable self tests after key generation.
end
```

system fm

Introduction.

```
config system fm
  set status { enable | disable }  Enable/disable FM.
  set id { string }  ID. size[35]
  set ip { ipv4 address }  IP address.
  set vdom { string }  VDOM. size[31] - datasource(s): system.vdom.name
  set auto-backup { enable | disable }  Enable/disable automatic backup.
  set scheduled-config-restore { enable | disable }  Enable/disable scheduled configuration restore.
  set ipsec { enable | disable }  Enable/disable IPsec.
end
```

system fortiguard

Introduction.

```
config system fortiguard
  set port { 53 | 8888 | 80 }  Port used to communicate with the FortiGuard servers.
    53    UDP Port 53 for server communication (for use by FortiGuard or FortiManager).
    8888  UDP Port 8888 for server communication (for use by FortiGuard or FortiManager).
    80    TCP Port 80 for server communication (for use only by FortiManager).
  set service-account-id { string }  Service account ID. size[50]
  set load-balance-servers { integer }  Number of servers to alternate between as first FortiGuard option. range[1-266]
  set antispam-force-off { enable | disable }  Enable/disable turning off the FortiGuard antispam service.
  set antispam-cache { enable | disable }  Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.
  set antispam-cache-ttl { integer }  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. range[300-86400]
  set antispam-cache-mpercent { integer }  Maximum percent of FortiGate memory the antispam cache is allowed to use (1 - 15%). range[1-15]
  set antispam-license { integer }  Interval of time between license checks for the FortiGuard antispam contract. range[0-4294967295]
  set antispam-expiration { integer }  Expiration date of the FortiGuard antispam contract. range[0-4294967295]
  set antispam-timeout { integer }  Antispam query time out (1 - 30 sec, default = 7). range[1-30]
  set avquery-cache-ttl { integer }  Time-to-live for antivirus cache entries (300 - 86400 sec, default = 1800).
  set avquery-cache-mpercent { integer }  Maximum percent of memory the antivirus cache can use (1 - 15%, default = 2).
  set avquery-license { integer }  Interval of time between license checks for the FortiGuard antivirus contract.
  set avquery-timeout { integer }  Antivirus query time out (1 - 30 sec, default = 7).
  set webfilter-force-off { enable | disable }  Enable/disable turning off the FortiGuard web filtering service.
  set webfilter-cache { enable | disable }  Enable/disable FortiGuard web filter caching.
  set webfilter-cache-ttl { integer }  Time-to-live for web filter cache entries in seconds (300 - 86400). range[300-86400]
  set webfilter-license { integer }  Interval of time between license checks for the FortiGuard web filter contract. range[0-4294967295]
  set webfilter-expiration { integer }  Expiration date of the FortiGuard web filter contract. range[0-4294967295]
  set webfilter-timeout { integer }  Web filter query time out (1 - 30 sec, default = 7). range[1-30]
  set sdns-server-ip { string }  IP address of the FortiDNS server.
  set sdns-server-port { integer }  Port used to communicate with FortiDNS servers. range[1-65535]
  set source-ip { ipv4 address }  Source IPv4 address used to communicate with FortiGuard.
  set source-ip6 { ipv6 address }  Source IPv6 address used to communicate with FortiGuard.
  set ddns-server-ip { ipv4 address }  IP address of the FortiDDNS server.
  set ddns-server-port { integer }  Port used to communicate with FortiDDNS servers. range[1-65535]
end
```

system fortimanager

Introduction.

```
config system fortimanager
  set ip { ipv4 address any }   IP address.
  set vdom { string }          Virtual domain name. size[31] - datasource(s): system.vdom.name
  set ipsec { enable | disable }  Enable/disable FortiManager IPsec tunnel.
  set central-management { enable | disable }  Enable/disable FortiManager central management.
  set central-mgmt-auto-backup { enable | disable }  Enable/disable central management auto backup.
  set central-mgmt-schedule-config-restore { enable | disable }  Enable/disable central management schedule config restore.
  set central-mgmt-schedule-script-restore { enable | disable }  Enable/disable central management schedule script restore.
end
```


system fortisandbox

Introduction.

```
config system fortisandbox
  set status { enable | disable }  Enable/disable FortiSandbox.
  set server { ipv4 address any }  Server IP.
  set source-ip { ipv4 address }  Source IP address for communications to FortiSandbox.
  set enc-algorithm { default | high | low | disable }  Configure the level of SSL protection for secure communication with FortiSandbox.
    default  SSL communication with high and medium encryption algorithms.
    high     SSL communication with high encryption algorithms.
    low      SSL communication with low encryption algorithms.
    disable  Disable SSL communication.
  set email { string }  Notifier email address. size[63]
end
```

system fssso-polling

Introduction.

```
config system fssso-polling
  set status { enable | disable }  Enable/disable FSSO Polling Mode.
  set listening-port { integer }  Listening port to accept clients (1 - 65535). range[1-65535]
  set authentication { enable | disable }  Enable/disable FSSO Agent Authentication.
  set auth-password { password_string }  Password to connect to FSSO Agent. size[128]
end
```

system ftm-push

Introduction.

```
config system ftm-push
  set server-port { integer }  Port to communicate with FortiToken Mobile push services server (1 - 65535, default = 4433). range[1-65535]
  set server-ip { ipv4 address }  IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).
  set status { enable | disable }  Enable/disable the use of FortiToken Mobile push services.
end
```

system geoip-override

Introduction.

```
config system geoip-override
  edit { name }
  # Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.
  set name { string } Location name. size[63]
  set description { string } Description. size[127]
  set country-id { string } Two character Country ID code. size[2]
  config ip-range
    edit { id }
    # Table of IP ranges assigned to country.
    set id { integer } ID number for individual entry in the IP-Range table. range[0-65535]
    set start-ip { ipv4 address } Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).
    set end-ip { ipv4 address } Final IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).
  next
next
end
```

system global

Use this command to configure global settings that affect FortiGate systems and configurations.

```
config system global
  set language { option } GUI display language.
    english English.
    french French.
    spanish Spanish.
    portuguese Portuguese.
    japanese Japanese.
    trach Traditional Chinese.
    simch Simplified Chinese.
    korean Korean.
  set gui-ipv6 { enable | disable } Enable/disable IPv6 settings on the GUI.
  set gui-certificates { enable | disable } Enable/disable the System } Certificate GUI page, allowing you to add and configure certificates from the GUI.
  set gui-custom-language { enable | disable } Enable/disable custom languages in GUI.
  set gui-wireless-opensecurity { enable | disable } Enable/disable wireless open security option on the GUI.
  set gui-display-hostname { enable | disable } Enable/disable displaying the FortiGate's hostname on the GUI login page.
  set gui-lines-per-page { integer } Number of lines to display per page for web administration. range[20-1000]
  set admin-https-ssl-versions { tlsv1-0 | tlsv1-1 | tlsv1-2 | sslv3 } Allowed SSL/TLS versions for web administration.
    tlsv1-0 TLS 1.0.
    tlsv1-1 TLS 1.1.
    tlsv1-2 TLS 1.2.
    sslv3 SSLv3.
  set admintimeout { integer } Number of minutes before an idle administrator session times out (5 - 480 minutes (8 hours), default = 5). A shorter idle timeout is more secure. range[1-480]
  set admin-console-timeout { integer } Console login timeout that overrides the admintimeout value. (15 - 300 seconds) (15 seconds to 5 minutes). 0 the default, disables this timeout. range[15-300]
  set ssd-trim-freq { option } How often to run SSD Trim (default = weekly). SSD Trim prevents SSD drive data loss by finding and isolating errors.
    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.
  set ssd-trim-hour { integer } Hour of the day on which to run SSD Trim (0 - 23, default = 1). range[0-23]
  set ssd-trim-min { integer } Minute of the hour on which to run SSD Trim (0 - 59, 60 for random). range[0-60]
  set ssd-trim-weekday { option } Day of week to run SSD Trim. Blank by default.
```

```
    sunday    Sunday
    monday    Monday
    tuesday   Tuesday
    wednesday Wednesday
    thursday  Thursday
    friday    Friday
    saturday  Saturday
set ssid-trim-date { integer } Date within a month to run ssd trim. range[1-31]
set admin-concurrent { enable | disable } Enable/disable concurrent administrator logins. (Use policy-auth-concurrent for firewall authenticated users.)
set admin-lockout-threshold { integer } Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration. range[1-10]
set admin-lockout-duration { integer } Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts. range[1-2147483647]
set refresh { integer } Statistics refresh interval in GUI. range[0-4294967295]
set interval { integer } Dead gateway detection interval. range[0-4294967295]
set failtime { integer } Fail-time for server lost. range[0-4294967295]
set daily-restart { enable | disable } Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.
set restart-time { string } Daily restart time (hh:mm).
set radius-port { integer } RADIUS service port number. range[1-65535]
set admin-login-max { integer } Maximum number of administrators who can be logged in at the same time (1 - 100, default = 100) range[1-100]
set remoteauthtimeout { integer } 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). range[1-300]
set ldapconntimeout { integer } Global timeout for connections with remote LDAP servers in milliseconds (0 - 4294967295, default 500). range[0-4294967295]
set batch-cmdb { enable | disable } Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.
set max-dlpstat-memory { integer } Maximum DLP stat memory (0 - 4294967295).
set dst { enable | disable } Enable/disable daylight saving time.
set timezone { option } 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.
    01 (GMT-11:00) Midway Island, Samoa
    02 (GMT-10:00) Hawaii
    03 (GMT-9:00) Alaska
    04 (GMT-8:00) Pacific Time (US & Canada)
    05 (GMT-7:00) Arizona
    81 (GMT-7:00) Baja California Sur, Chihuahua
    06 (GMT-7:00) Mountain Time (US & Canada)
    07 (GMT-6:00) Central America
    08 (GMT-6:00) Central Time (US & Canada)
    09 (GMT-6:00) Mexico City
    10 (GMT-6:00) Saskatchewan
```

```
11 (GMT-5:00) Bogota, Lima,Quito
12 (GMT-5:00) Eastern Time (US & Canada)
13 (GMT-5:00) Indiana (East)
74 (GMT-4:00) Caracas
14 (GMT-4:00) Atlantic Time (Canada)
77 (GMT-4:00) Georgetown
15 (GMT-4:00) La Paz
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
87 (GMT-3:00) Paraguay
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
26 (GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
27 (GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
28 (GMT+1:00) Brussels, Copenhagen, Madrid, Paris
78 (GMT+1:00) Namibia
29 (GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb
30 (GMT+1:00) West Central Africa
31 (GMT+2:00) Athens, Sofia, Vilnius
32 (GMT+2:00) Bucharest
33 (GMT+2:00) Cairo
34 (GMT+2:00) Harare, Pretoria
35 (GMT+2:00) Helsinki, Riga, Tallinn
36 (GMT+2:00) Jerusalem
37 (GMT+3:00) Baghdad
38 (GMT+3:00) Kuwait, Riyadh
83 (GMT+3:00) Moscow
84 (GMT+3:00) Minsk
40 (GMT+3:00) Nairobi
85 (GMT+3:00) Istanbul
41 (GMT+3:30) Tehran
42 (GMT+4:00) Abu Dhabi, Muscat
43 (GMT+4:00) Baku
39 (GMT+3:00) St. Petersburg, Volgograd
```

```
44 (GMT+4:30) Kabul
46 (GMT+5:00) Islamabad, Karachi, Tashkent
47 (GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi
51 (GMT+5:30) Sri Jayawardenepara
48 (GMT+5:45) Kathmandu
45 (GMT+5:00) Ekaterinburg
49 (GMT+6:00) Almaty, Novosibirsk
50 (GMT+6:00) Astana, Dhaka
52 (GMT+6:30) Rangoon
53 (GMT+7:00) Bangkok, Hanoi, Jakarta
54 (GMT+7:00) Krasnoyarsk
55 (GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk
56 (GMT+8:00) Ulaan Bataar
57 (GMT+8:00) Kuala Lumpur, Singapore
58 (GMT+8:00) Perth
59 (GMT+8:00) Taipei
60 (GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
62 (GMT+9:30) Adelaide
63 (GMT+9:30) Darwin
61 (GMT+9:00) Yakutsk
64 (GMT+10:00) Brisbane
65 (GMT+10:00) Canberra, Melbourne, Sydney
66 (GMT+10:00) Guam, Port Moresby
67 (GMT+10:00) Hobart
68 (GMT+10:00) Vladivostok
69 (GMT+10:00) Magadan
70 (GMT+11:00) Solomon Is., New Caledonia
71 (GMT+12:00) Auckland, Wellington
72 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
00 (GMT+12:00) Niue, Tokelau
82 (GMT+12:45) Chatham Islands
73 (GMT+13:00) Nuku'alofa
86 (GMT+13:00) Samoa
76 (GMT+14:00) Kiritimati

set ntpserver { string } IP address or hostname of the NTP Server. size[63]
set ntpsync { enable | disable } Enable/disable synchronization with NTP Server.
set syncinterval { integer } NTP synchronization interval (1 - 1440 min). range[1-1440]
set traffic-priority { tos | dscp } Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in
traffic shaping.
    tos IP TOS.
    dscp DSCP (DiffServ) DS.
set traffic-priority-level { low | medium | high } Default system-wide level of priority for traffic prioritization.
    low Low priority.
```



```
    medium Medium priority.
    high High priority.
set anti-replay { disable | loose | strict } Level of checking for packet replay and TCP sequence checking.
    disable Disable anti-replay check.
    loose Loose anti-replay check.
    strict Strict anti-replay check.
set send-pmtu-icmp { enable | disable } 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.
set honor-df { enable | disable } Enable/disable honoring of Don't-Fragment (DF) flag.
set revision-image-auto-backup { enable | disable } Enable/disable back-up of the latest configuration revision after the firmware is upgraded.
set revision-backup-on-logout { enable | disable } Enable/disable back-up of the latest configuration revision when an administrator logs out
of the CLI or GUI.
set management-vdom { string } Management virtual domain name. size[31] - datasource(s): system.vdom.name
set hostname { string } FortiGate unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up
to 35 characters. size[35]
set alias { string } Alias for your FortiGate unit. size[35]
set strong-crypto { enable | disable } Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for
HTTPS/SSH admin access.
set ssh-cbc-cipher { enable | disable } Enable/disable CBC cipher for SSH access.
set ssh-hmac-md5 { enable | disable } Enable/disable HMAC-MD5 for SSH access.
set ssl-static-key-ciphers { enable | disable } Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-
SHA256, AES256-SHA256).
set snat-route-change { enable | disable } Enable/disable the ability to change the static NAT route.
set cli-audit-log { enable | disable } Enable/disable CLI audit log.
set dh-params { option } Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.
    1024 1024 bits.
    1536 1536 bits.
    2048 2048 bits.
    3072 3072 bits.
    4096 4096 bits.
    6144 6144 bits.
    8192 8192 bits.
set fds-statistics { enable | disable } 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.
set fds-statistics-period { integer } FortiGuard statistics collection period in minutes. (1 - 1440 min (1 min to 24 hours), default = 60).
range[1-1440]
set multicast-forward { enable | disable } Enable/disable multicast forwarding.
set mc-ttl-notchange { enable | disable } Enable/disable no modification of multicast TTL.
set asymroute { enable | disable } Enable/disable asymmetric route.
set tcp-option { enable | disable } Enable SACK, timestamp and MSS TCP options.
set lldp-transmission { enable | disable } Enable/disable Link Layer Discovery Protocol (LLDP) transmission.
set proxy-auth-timeout { integer } Authentication timeout in seconds for idle explicit web proxy sessions. range[1-600]
set sys-perf-log-interval { integer } Time in minutes between updates of performance statistics logging. (1 - 15 min, default = 5, 0 =
```

```
disabled). range[0-15]
  set check-protocol-header { loose | strict } Level of checking performed on protocol headers. Strict checking is more thorough but may affect
performance. Loose checking is ok in most cases.
    loose Check protocol header loosely.
    strict Check protocol header strictly.
  set vip-arp-range { unlimited | restricted } Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.
    unlimited Send ARPs for all addresses in VIP range.
    restricted Send ARPs for the first 8192 addresses in VIP range.
  set reset-sessionless-tcp { enable | disable } Action to perform if the FortiGate receives a TCP packet but cannot find a corresponding session
in its session table. NAT/Route mode only.
  set allow-traffic-redirect { enable | disable } Disable to allow traffic to be routed back on a different interface.
  set strict-dirty-session-check { enable | disable } 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.
  set tcp-halfclose-timer { integer } 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). range[1-86400]
  set tcp-halfopen-timer { integer } 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). range[1-86400]
  set tcp-timewait-timer { integer } Length of the TCP TIME-WAIT state in seconds. range[0-300]
  set udp-idle-timer { integer } UDP connection session timeout. This command can be useful in managing CPU and memory resources (1 - 86400
seconds (1 day), default = 60). range[1-86400]
  set block-session-timer { integer } Duration in seconds for blocked sessions (1 - 300 sec (5 minutes), default = 30). range[1-300]
  set ip-src-port-range { string } IP source port range used for traffic originating from the FortiGate unit.
  set pre-login-banner { enable | disable } Enable/disable displaying the administrator access disclaimer message on the login page before an
administrator logs in.
  set post-login-banner { disable | enable } Enable/disable displaying the administrator access disclaimer message after an administrator suc-
cessfully logs in.
  set tftp { enable | disable } Enable/disable TFTP.
  set av-failopen { pass | off | one-shot } Set the action to take if the FortiGate is running low on memory or the proxy connection limit has
been reached.
    pass Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.
    off Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.
    one-shot Bypass the antivirus system when memory is low.
  set av-failopen-session { enable | disable } 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.
  set memory-use-threshold-extreme { integer } Threshold at which memory usage is considered extreme (new sessions are dropped) (% of total RAM,
default = 95). range[70-97]
  set memory-use-threshold-red { integer } Threshold at which memory usage forces the FortiGate to enter conserve mode (% of total RAM, default =
88). range[70-97]
  set memory-use-threshold-green { integer } Threshold at which memory usage forces the FortiGate to exit conserve mode (% of total RAM, default
= 82). range[70-97]
  set check-reset-range { strict | disable } Configure ICMP error message verification. You can either apply strict RST range checking or disable
it.
```

```
    strict    Check RST range strictly.
    disable  Disable RST range check.
set vdom-admin { enable | disable } Enable/disable support for multiple virtual domains (VDOMs).
set long-vdom-name { enable | disable } Enable/disable long VDOM name support.
set admin-port { integer } Administrative access port for HTTP. (1 - 65535, default = 80). range[1-65535]
set admin-sport { integer } Administrative access port for HTTPS. (1 - 65535, default = 443). range[1-65535]
set admin-https-redirect { enable | disable } Enable/disable redirection of HTTP administration access to HTTPS.
set admin-ssh-password { enable | disable } Enable/disable password authentication for SSH admin access.
set admin-ssh-port { integer } Administrative access port for SSH. (1 - 65535, default = 22). range[1-65535]
set admin-ssh-grace-time { integer } Maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating (10 - 3600 sec (1 hour), default 120). range[10-3600]
set admin-ssh-v1 { enable | disable } Enable/disable SSH v1 compatibility.
set admin-telnet-port { integer } Administrative access port for TELNET. (1 - 65535, default = 23). range[1-65535]
set admin-maintainer { enable | disable } 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.
set admin-server-cert { string } Server certificate that the FortiGate uses for HTTPS administrative connections. size[35] - datasource(s): certificate.local.name
set user-server-cert { string } Certificate to use for https user authentication. size[35] - datasource(s): certificate.local.name
set admin-https-pki-required { enable | disable } 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.
set allow-empty-passwords { enable | disable } Allow or prohibit the use of empty passwords for local administrators.
set wifi-certificate { string } Certificate to use for WiFi authentication. size[35] - datasource(s): certificate.local.name
set wifi-ca-certificate { string } CA certificate that verifies the WiFi certificate. size[35] - datasource(s): certificate.ca.name
set auth-http-port { integer } User authentication HTTP port. (1 - 65535, default = 80). range[1-65535]
set auth-https-port { integer } User authentication HTTPS port. (1 - 65535, default = 443). range[1-65535]
set auth-keepalive { enable | disable } Enable to prevent user authentication sessions from timing out when idle.
set policy-auth-concurrent { integer } Number of concurrent firewall use logins from the same user (1 - 100, default = 0 means no limit). range[0-100]
set auth-session-limit { block-new | logout-inactive } Action to take when the number of allowed user authenticated sessions is reached.
    block-new    Block new user authentication attempts.
    logout-inactive Logout the most inactive user authenticated sessions.
set auth-cert { string } Server certificate that the FortiGate uses for HTTPS firewall authentication connections. size[35] - datasource(s): certificate.local.name
set clt-cert-req { enable | disable } Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.
set fortiservice-port { integer } FortiService port (1 - 65535, default = 8013). Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port. range[1-65535]
set endpoint-control-portal-port { integer } Endpoint control portal port (1 - 65535). range[1-65535]
set endpoint-control-fds-access { enable | disable } Enable/disable access to the FortiGuard network for non-compliant endpoints.
set tp-mc-skip-policy { enable | disable } Enable/disable skip policy check and allow multicast through.
set cfg-save { automatic | manual | revert } Configuration file save mode for CLI changes.
    automatic  Automatically save config.
    manual     Manually save config.
```

```
    revert      Manually save config and revert the config when timeout.
set cfg-revert-timeout { integer }  Time-out for reverting to the last saved configuration. range[10-4294967295]
set reboot-upon-config-restore { enable | disable }  Enable/disable reboot of system upon restoring configuration.
set admin-scp { enable | disable }  Enable/disable using SCP to download the system configuration. You can use SCP as an alternative method for
backing up the configuration.
set wireless-controller { enable | disable }  Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.
set wireless-controller-port { integer }  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). range[1024-49150]
set fortiextender-data-port { integer }  FortiExtender data port (1024 - 49150, default = 25246). range[1024-49150]
set fortiextender { enable | disable }  Enable/disable FortiExtender.
set fortiextender-vlan-mode { enable | disable }  Enable/disable FortiExtender VLAN mode.
set switch-controller { disable | enable }  Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from
the FortiGate itself.
set switch-controller-reserved-network { ipv4 classnet }  Enable reserved network subnet for controlled switches. This is available when the
switch controller is enabled.
set proxy-worker-count { integer }  Proxy worker count. range[1-12]
set scanunit-count { integer }  Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units
with multiple CPUs. range[2-12]
set proxy-kxp-hardware-acceleration { disable | enable }  Enable/disable using the content processor to accelerate KXP traffic.
set proxy-cipher-hardware-acceleration { disable | enable }  Enable/disable using content processor (CP8 or CP9) hardware acceleration to
encrypt and decrypt IPsec and SSL traffic.
set fgd-alert-subscription { option }  Type of alert to retrieve from FortiGuard.
    advisory      Retrieve FortiGuard advisories, report and news alerts.
    latest-threat  Retrieve latest FortiGuard threats alerts.
    latest-virus   Retrieve latest FortiGuard virus alerts.
    latest-attack  Retrieve latest FortiGuard attack alerts.
    new-antivirus-db  Retrieve FortiGuard AV database release alerts.
    new-attack-db  Retrieve FortiGuard IPS database release alerts.
set ipsec-hmac-offload { enable | disable }  Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.
set ipv6-accept-dad { integer }  Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD). range[0-2]
set ipv6-allow-anycast-probe { enable | disable }  Enable/disable IPv6 address probe through Anycast.
set csr-ca-attribute { enable | disable }  Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attrib-
ute.
set wimax-4g-usb { enable | disable }  Enable/disable comparability with WiMAX 4G USB devices.
set cert-chain-max { integer }  Maximum number of certificates that can be traversed in a certificate chain. range[1-2147483647]
set sslvpn-max-worker-count { integer }  Maximum number of SSL VPN processes. Upper limit for this value is the number of CPUs and depends on
the model. range[1-12]
set sslvpn-kxp-hardware-acceleration { enable | disable }  Enable/disable SSL VPN KXP hardware acceleration.
set sslvpn-cipher-hardware-acceleration { enable | disable }  Enable/disable SSL VPN hardware acceleration.
set sslvpn-plugin-version-check { enable | disable }  Enable/disable checking browser's plugin version by SSL VPN.
set two-factor-ftk-expiry { integer }  FortiToken authentication session timeout (60 - 600 sec (10 minutes), default = 60). range[60-600]
set two-factor-email-expiry { integer }  Email-based two-factor authentication session timeout (30 - 300 seconds (5 minutes), default = 60).
range[30-300]
```

```
set two-factor-sms-expiry { integer } SMS-based two-factor authentication session timeout (30 - 300 sec, default = 60). range[30-300]
set two-factor-fac-expiry { integer } FortiAuthenticator token authentication session timeout (10 - 3600 seconds (1 hour), default = 60). range
[10-3600]
set two-factor-ftm-expiry { integer } FortiToken Mobile session timeout (1 - 168 hours (7 days), default = 72). range[1-168]
set per-user-bwl { enable | disable } Enable/disable per-user black/white list filter.
set virtual-server-count { integer } Maximum number of virtual server processes to create. The maximum is the number of CPU cores. This is not
available on single-core CPUs. range[1-12]
set virtual-server-hardware-acceleration { disable | enable } Enable/disable virtual server hardware acceleration.
set wad-worker-count { integer } Number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy
and web caching is handled by half of the CPU cores in a FortiGate unit. range[1-12]
set login-timestamp { enable | disable } Enable/disable login time recording.
set miglogd-children { integer } 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. range[0-15]
set special-file-23-support { disable | enable } Enable/disable IPS detection of HIBUN format files when using Data Leak Protection.
set log-uuid { disable | policy-only | extended } Whether UUIDs are added to traffic logs. You can disable UUIDs, add firewall policy UUIDs to
traffic logs, or add all UUIDs to traffic logs.
    disable      Disable UUID in traffic log
    policy-only  Enable only policy UUID in traffic log.
    extended     Enable all UUIDs in traffic log.
set log-ssl-connection { enable | disable } Enable/disable logging of SSL connection events.
set arp-max-entry { integer } Maximum number of dynamically learned MAC addresses that can be added to the ARP table (131072 - 2147483647,
default = 131072). range[131072-2147483647]
set ips-affinity { string } Affinity setting for IPS (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxxx; allowed CPUs must be less
than total number of IPS engine daemons). size[19]
set av-affinity { string } Affinity setting for AV scanning (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxxx). size[19]
set miglog-affinity { string } Affinity setting for logging (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxxx). size[19]
set wad-affinity { string } Affinity setting for wad (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxxx). size[19]
set ndp-max-entry { integer } Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries). range
[65536-2147483647]
set br-fdb-max-entry { integer } Maximum number of bridge forwarding database (FDB) entries. range[8192-2147483647]
set max-route-cache-size { integer } Maximum number of IP route cache entries (0 - 2147483647). range[0-2147483647]
set ipsec-asic-offload { enable | disable } Enable/disable ASIC offloading (hardware acceleration) for IPsec VPN traffic. Hardware acceleration
can offload IPsec VPN sessions and accelerate encryption and decryption.
set device-idle-timeout { integer } 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). range[30-31536000]
set device-identification-active-scan-delay { integer } Number of seconds to passively scan a device before performing an active scan. (20 -
3600 sec, (20 sec to 1 hour), default = 90). range[20-3600]
set compliance-check { enable | disable } Enable/disable global PCI DSS compliance check.
set compliance-check-time { time } Time of day to run scheduled PCI DSS compliance checks.
set gui-device-latitude { string } Add the latitude of the location of this FortiGate to position it on the Threat Map. size[19]
set gui-device-longitude { string } Add the longitude of the location of this FortiGate to position it on the Threat Map. size[19]
set private-data-encryption { disable | enable } Enable/disable private data encryption using an AES 128-bit key.
set auto-auth-extension-device { enable | disable } Enable/disable automatic authorization of dedicated Fortinet extension devices.
```

```
set gui-theme { option } Color scheme for the administration GUI.
    green      Green theme.
    red        Red theme.
    blue       Light blue theme.
    melongene  Melongene theme (eggplant color).
    mariner    Mariner theme (dark blue color).
set igmp-state-limit { integer } Maximum number of IGMP memberships (96 - 64000, default = 3200). range[96-128000]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

admin-concurrent {enable | disable}

Enable/disable to allow concurrent administrator logins. Default is `enable`. Use `policy-auth-concurrent` for firewall authenticated users.

admin-console-timeout <secs_int>

Specify a console login timeout that overrides the `admintimeout` value. Range: 15 - 300 seconds (15 seconds to 5 minutes). Zero value disables the timeout. Default is 0.

admin-https-pki-required {enable | disable}

Specify admin login method for HTTPS login. Default is `disable`.

- `enable`: allows admin user to log in by providing a valid certificate if PKI is enabled for HTTPS administrative access.
- `disable`: allows admin users to log in by providing a valid certificate or password.

admin-https-redirect {enable | disable}

Enable/disable redirection of HTTP administration access to HTTPS. Not available on low-crypto FortiGates. Default is `disable`.

admin-https-ssl-versions {sslv3 | tlsv1-0 | tlsv1-1 | tlsv1-2}

Specify allowed SSL/TLS versions for web administration. Default is `tlsv1-1 tlsv1-2`.

admin-lockout-duration <time_int>

Set the administration account's lockout duration in seconds for the firewall. Repeated failed login attempts will enable the lockout. Use `admin-lockout-threshold` to set the number of failed attempts that will trigger the lockout. Default is 60.

admin-lockout-threshold <failed_int>

Set the number of failed attempts before the account is locked out for the `admin-lockout-duration`. Default is . Default is 3.

admin-login-max <int>

Set the maximum number administrators who can be logged in at same time. Range: 1 - 100. Default is 80.

admin-maintainer {enable | disable}

Enable/disable hidden maintainer user login. Default is `enable`. 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.

admin-port <port_number>

Specify the administrative access port for HTTP. Range: 1 - 65535. Default is 80.

admin-scp {enable | disable}

Enable/disable allow system configuration download by secure copy protocol (SCP). You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for an administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. Default is `disable`. To backup a VDOM configuration:

```
config global
    set admin-scp enable
end
config vdom
edit <vdom_name>
```

admin-server-cert {self-sign | <certificate>}

Identify the admin HTTPS server certificate to use. Default is `self-sign`.

admin-sport <port_number>

Specify the administrative access port for HTTPS. Range: 1 - 65535. Default is 443.

admin-ssh-grace-time <time_int>

Specify the maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating. Range: 10 - 3600 seconds (10 seconds to one hour). Default is 120.

admin-ssh-password {enable | disable}

Enable/disable password authentication for SSH admin access. Default is `enable`.

admin-ssh-port <port_number>

Specify the administrative access port for SSH. Range: 1 - 65535. Default is 22.

admin-ssh-v1 {enable | disable}

Enable/disable Secure Shell (SSH) version 1 compatibility. Default is `disable`.

admin-telnet-port <port_number>

Specify the administrative access port for TELNET. Range: 1 - 65535. Default is 23.

admintimeout <admin_timeout_minutes>

Specify the number of minutes before an idle administrator times out. The maximum `admintimeout` interval is 480 minutes (8 hours). Default is 5. To improve security keep the idle timeout at the default value.

alias <alias_str>

Identify an alias for your FortiGate unit.

allow-traffic-redirect {enable | disable}

Enable/ disable allow traffic redirect. Default is `enable`. Under some conditions, it is undesirable to have traffic routed back on the same interface. In that case, set `allow-traffic-redirect` to `disable`.

anti-replay {disable | loose | strict}

Specify the level of checking for packet replay and TCP sequence checking (or TCP Sequence number checking). Default is `strict`. FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets.

- `disable`: no anti-replay protection.
- `loose`: perform packet sequence checking and ICMP anti-replay checking with the following criteria:
 - the SYN, FIN, and RST bit can not appear in the same packet.
 - the FortiGate unit does not allow more than 1 ICMP error packet to go through the FortiGate unit before it receives a normal TCP or UDP packet.
 - If the FortiGate unit receives an RST packet, and `check-reset-range` is set to `strict` the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
- `strict`: performs all of the loose checking but for each new session also checks to determine if the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding.

If any packet fails a check it is dropped. If `loginvalid-packet` is set to `enable`, a log message is written for each packet that fails a check.

arp-max-entry <int>

Specify the maximum number of dynamically learned MAC addresses that can be added to the ARP table. Range: 131072 - 2147483647. If set to 0, kernel holds 131072 entries. Default is 0.

auth-cert <cert-name>

Identify the HTTPS server certificate for policy authentication. Default is `self-sign`. `Self-sign` is the built-in certificate but others will be listed as you add them.

auth-http-port <http_port>

Set the HTTP authentication port. Range: 1 - 65535. Default is 1000.

auth-https-port <https_port>

Set the HTTPS authentication port. Range: 1 - 65535. Default is 1003.

auth-keepalive {enable | disable}

Enable to extend the session's authentication time to prevent an idle timeout. Default is `disable`.

auto-auth-extension-device {enable | disable}

Enable/disable automatic authorization of dedicated Fortinet extension device globally. Default is `enable`.

av-failopen {idledrop | off | one-shot | pass}

Set the action to take if the unit is running low on memory or the proxy connection limit has been reached. Default is `pass`.

- `idledrop`: drop connections based on the clients that have the most connections open. This is most useful for Windows applications, and can prevent malicious bots from keeping an idle connection open to a remote server.
- `off`: stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.
- `one-shot`: bypass the antivirus system when memory is low. You must enter `off` or `pass` to restart antivirus scanning.
- `pass`: bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved

av-failopen-session {enable | disable}

When enabled and a protocol's proxy runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by `av-failopen`. Default is `disable`.

batch-cmdb {enable | disable}

Enable/disable batch mode to execute in CMDB server. Batch mode is used to enter a series of commands that will execute as a group once they are loaded. Default is `enable`.

block-session-timer <int>

Set the time duration in seconds for blocked sessions. Range: 1 - 300 seconds (1 second to 5 minutes). Default is 30.

br-fdb-max-entry <int>

Specify the maximum number of bridge forwarding database (FDB) entries. Used when operating in Transparent mode, the FDB (or MAC) table is used by a Layer 2 device (switch/bridge) to store MAC addresses that have been learned and the ports that each MAC address was learned on. If the FDB has a large

number of entries, performance may be impacted. Range: 8192 - 2147483647. If set to 0, kernel holds 8192 entries. Default is 0.

cert-chain-max <int>

Set the maximum number of certificates that can be traversed in a certificate chain. The list of certificates, from the root certificate to the end-user certificate, represents the certificate chain. Default is 8.

cfg-save {automatic | manual | revert}

Specify the configuration file save mode for changes made using the CLI. Default is `automatic`.

- `automatic`: automatically save the configuration after every change.
- `manual`: manually save the configuration using the `execute cfg save` command.
- `revert`: manually save the current configuration and then revert to that saved configuration after `cfg-revert-timeout` expires.

Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode. [/expand]

check-protocol-header {loose | strict}

Select the level of checking performed on protocol headers. Default is `loose`.

- `loose`: the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc.
- `strict`: the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length. Note: this setting disables hardware acceleration.

If the packet fails header checking it is dropped by the FortiGate unit and logged if `log-invalid-packet` is enabled.

check-reset-range {disable | strict}

Configure ICMP error message verification. Default is `disable`.

- `disable`: the FortiGate unit does not validate ICMP error messages.
- `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) |TCP(C,D) header and if FortiOS can locate the A:C->B:D session, it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range, then the ICMP packet is dropped. If `log-invalid-packet` is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets

cli-audit-log {enable | disable}

Enable/disable CLI audit log. Default is `disable`.

clt-cert-req {enable | disable}

Enable/disable requirement for a client certificate before administrator logs in via GUI using HTTPS. Default is `disable`.

compliance-check {enable | disable}

Enable/disable global PCI DSS compliance check. Default is `enable`.

compliance-check-time <HH:MM:SS>

Specify the PCI DSS compliance check time. Default is `00:00:00`.

csr-ca-attribute {enable | disable}

Enable/disable the use of CA attribute in your certificate. Some CA servers reject CSRs that have the CA attribute. Default is `enable`.

daily restart {enable | disable}

Enable/disable daily restart of FortiGate unit. Default is `disable`. The time of the restart is controlled by `restart-time`.

device-identification-active-scan-delay <int>

Indicate how many seconds to passively scan a device before performing an active scan. Range: 20 - 3600 seconds (20 seconds to 1 hour). Default is 90.

device-idle-timeout <int>

Specify time in seconds that a device must be idle in order to automatically log user out. Range: 30 - 31536000 seconds (30 seconds to 1 year). Default is 300.

dh-params {1024 | 1536 | 2048 | 3072 | 4096 | 6144 | 8192}

Minimum size, in bits, of the prime number used in Diffie-Hellman key exchange for HTTPS/SSH protocols. Default is 2048.

disk-usage {log | wanopt}

Specify whether to use hard disk or WAN Optimization for logging. Default is `log`.

dst {enable | disable}

Enable/disable daylight saving time. Default is `enable`.

endpoint-control-fds-access {enable | disable}

Enable/disable access to FortiGuard network for non-compliant endpoints. Default is `enable`.

endpoint-control-portal-port

Specify the endpoint control portal port. Range: 1 - 65535. Default is `8009`.

explicit-proxy-auth-timeout <int>

Specify authentication timeout in seconds for idle sessions in explicit web proxy. Default is `300`.

fds-statistics {enable | disable}

Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. Default is `enable`.

fds-statistics-period <int>

Indicate the FortiGuard statistics update period in minutes. Range: 1 - 1440 minutes (1 minute to 24 hours). Default is `60`.

fgd-alert-subscription {advisory | latest-threat | latest-virus | latest-attack | new-antivirus-db | new-attack-db}

Specify the type of alert to retrieve from FortiGuard.

- `advisory`: retrieves FortiGuard advisories, report, and news alerts.
- `latest-threat`: retrieves latest FortiGuard threat alerts.
- `latest-virus`: retrieves latest FortiGuard virus alerts.
- `latest-attack`: retrieves latest FortiGuard attack alerts.
- `new-antivirus-db`: retrieves latest FortiGuard antivirus database release alerts.
- `new attack-db`: retrieves latest FortiGuard IPS database release alerts.

fortiextender {enable | disable}

Enable/disable FortiExtender controller. Default is `disable`.

fortiextender-data-port <port_int>

Specify Fortiextender controller data port. Range: 1024 - 49150. Default is `25246`.

fortiservice-port <port_int>

Specify the FortiService port number. Default is `8013`.

Starting with FortiClient 5.4, endpoint compliance (EC) registration will use port 8013 by default. To register to FortiOS 5.0 or 5.2, the user must specify port 8010 with the IP address, separated by a colon. For example, `<IP_Address>:8010`. FortiOS 5.4 will listen on port 8013. If registering from FortiClient 5.4 to FortiOS 5.4, the default ports will match. Specifying the port number with the IP address is then optional. For more information, refer to [FortiClient 5.4.0 Release Notes](#) which is available in the [Fortinet Document Library](#).

gui-certificates {enable | disable}

Enable/disable certificate configuration in GUI. Default is `enable`.

gui-custom-language {enable | disable}

Enable/disable custom languages in GUI. Default is `disable`.

gui-device-latitude <string>

Identify the latitude coordinate of your FortiGate.

gui-device-longitude <string>

Identify the longitude coordinate of your FortiGate.

gui-display-hostname {enable | disable}

Enable/disable display of hostname on GUI login page. Default is `disable`.

gui-ipv6 {enable | disable}

Enable/disable IPv6 settings in GUI. Default is `disable`.

gui-lines-per-page <gui_lines>

Specify number of lines to display per page for web administration. Default is `50`.

gui-theme {green | red | blue | melongene | mariner}

Select color scheme to use for the administration GUI. Default is `green`.

gui-wireless-opensecurity {enable | disable}

Enable/disable wireless open security option in GUI. Default is `disable`.

honor-df {enable | disable}

Enable/disable honoring of Don't-Fragment (DF) flag. The DF flag instructs routers that would normally fragment a packet that is too large for a link's MTU (and potentially deliver it out of order due to that fragmentation) to instead drop the packet and return an ICMP Fragmentation Needed packet, allowing the sending host to account for the lower MTU on the path to the destination host. Default is `enable`.

hostname <unithostname>

Specify FortiGate unit hostname. Default is FortiGate serial number.

A hostname can only include letters, numbers, hyphens, and underlines. No spaces allowed.

While the hostname can be longer than 24 characters, if it is longer than 24 characters it will be truncated by a "~". The trailing 3-characters preceded by the "~" truncation character and the first N-3 characters are shown. This shortened hostname will be displayed in the CLI, and other locations the hostname is used. Some models support hostnames up to 35 characters

ip-src-port-range <start_port>-<end_port>

Specify the IP source port range used for traffic originating from the FortiGate unit. Range: 1-65535. Default is 1024-499. You can use this setting to avoid problems with networks that block some ports, such as FDN ports.

ips-affinity <string>

Affinity setting for IPS (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).

ipsec-asic-offload {enable | disable}

Enable/disable application-specific integrated circuit (ASIC) offload for IPsec VPN. You can use this command to disable using ASIC offloading to accelerate IPsec Diffie-Hellman key exchange for IPsec ESP traffic. By default hardware offloading is used. For debugging purposes or other reasons you may want this function to be processed by software. Default is `enable`.

ipsec-hmac-offload {disable | enable}

Enable/disable offload keyed-hashing for message authentication (HMAC) to hardware for IPsec VPN. Default is `enable`.

ipv6-accept-dad {0 | 1 | 2}

Enable/disable acceptance of IPv6 DAD (Duplicate Address Detection). 0: Disable DAD; 1: Enable DAD (default); 2: Enable DAD, and disable IPv6 operation if MAC-based duplicate link-local address has been found.

language <string>

Identify the GUI display language. `set language ?` lists available languages. `trach` = Traditional Chinese. `simch` = Simplified Chinese. Default is `english`.

ldapconntimeout <integer>

LDAP connection time-out in milliseconds. Range: 0 - 4294967295.

lldp-transmission {enable | disable}

Enable/disable Link Layer Discovery Protocol (LLDP) transmission. Default is `disable`.

log-uuid {disable | policy-only | extended}

Universally Unique Identifier (UUID) log option. Default is `policy-only`.

login-timestamp {enable | disable}

Enable/disable login time recording. Default is `disable`.

management-vdom <domain>

Management virtual domain name. Default is `root`.

max-route-cache-size <int>

Specify the maximum number of IP route cache entries. Range: 0 - 2 147483647. Default is 0.

miglog-affinity

Affinity setting for logging (64-bit hexadecimal value in the format of `xxxxxxxxxxxxxxxx`).

miglogd-children <int>

Specify the number of miglogd processes to run. A higher number can affect performance, and a lower number can affect log processing time, although no logs will be dropped or lost if the number is decreased. If you are suffering from performance issues, you can alter the number of logging daemon child processes. Range: 0 - 15. Default is 0.

ndp-max-entry <int>

Specify the maximum number of Neighbor Discovery Protocol (NDP) table entries. Set to 65,536 or higher; if set to 0, kernel holds 65,536 entries. Default is 0. Specify the maximum number of Neighbor Discovery Protocol (NDP) table entries. Set to 65,536 or higher; if set to 0, kernel holds 65,536 entries. Default is 0.

optimize {antivirus}

DO NOT USE THIS COMMAND. It was originally added to early NP4 platforms but is no longer supported.

phase1-rekey {enable | disable}

Enable/disable rekeying between Internet Key Exchange (IKE) peers before the phase 1 keylife expires. Default is `enable`.

policy-auth-concurrent <limit_int>

Limit the number of concurrent logins from the same user. Range: 1 - 100. Default is 0 and means no limit.

post-login-banner {enable | disable}

Enable/disable to display the admin access disclaimer message after successful login. Default is `disable`.

pre-login-banner {enable | disable}

Enable/disable to display the admin access disclaimer prior to login. Default is `disable`.

private-data-encryption {enable | disable}

Enable/disable private data encryption using an AES 128-bit key. Default is `disable`.

proxy-cipher-hardware-acceleration {enable | disable}

Enable/disable use of content processor to encrypt or decrypt traffic. Default is `enable`.

proxy-kxp-hardware-acceleration {enable | disable}

Enable/disable use of content processor to encrypt or decrypt traffic. Default is `enable`.

proxy-worker-count <count_int>

Specify the number of proxy worker processes. Range: 1 - 8. Default is 4.

radius-port <radius_port>

Specify the port for RADIUS traffic. Default is 1812. If your RADIUS server is using port 1645, you can use the CLI to change the RADIUS port on your FortiGate unit.

reboot-upon-config-restore {enable | disable}

Enable/disable reboot of system when restoring configuration. Default is `enable`.

refresh <refresh_seconds>

Specify the Automatic Refresh Interval, in seconds, for GUI statistics. Range: 0-4294967295. Default is 0, or no automatic refresh.

registration-notification {enable | disable}

Enable/disable displaying the registration notification if the FortiGate is not registered. Default is `enable`.

remoteauthtimeout <timeout_sec>

Specify the number of seconds that the FortiGate unit waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. Range: 0-300 seconds, 0 means no timeout. Default is 5. To improve security keep the remote authentication timeout at the default value of 5 seconds. However, if a RADIUS request needs to traverse multiple hops or several RADIUS requests are made, the default timeout of 5 seconds may not be long enough to receive a response.

reset-sessionless-tcp {enable | disable}

The `reset-sessionless-tcp` command determines what action the FortiGate unit performs if it receives a TCP packet but cannot find a corresponding session in its session table. This happens most often because the session has timed out. In most cases you should leave `reset-sessionless-tcp` set to `disable` (the default). When this command is set to `disable`, the FortiGate unit silently drops the packet. The packet originator does not know that the session has expired and might re-transmit the packet several times before attempting to start a new session. Enabling this option may help resolve issues with a problematic server, but it can make the FortiGate unit more vulnerable to denial of service attacks. If you enable `reset-sessionless-tcp`, the FortiGate unit sends a RESET packet to the packet originator. The packet originator ends the current session, but it can try to establish a new session. Available in NAT/Route mode only. Default is `disable`.

revision-backup-on-logout {enable | disable}

Enable/disable back-up of the latest configuration revision when the administrator logs out of the CLI or GUI. Default is `disable`.

revision-image-auto-backup {enable | disable}

Enable/disable back-up of the latest configuration revision when firmware is upgraded. Default is `disable`.

scanunit-count <count_int>

Tune the number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs. Recommended for advanced users.

send-pmtu-icmp {enable | disable}

Enable to send a path maximum transmission unit (PMTU) - ICMP destination unreachable packet and to support PMTUD protocol on your network to reduce fragmentation of packets. Disabling this command will result in PMTUD packets being blocked. Default is `enable`.

service-expire-notification {enable | disable}

Enable/disable display of a 30-day notice of support contract expiry on GUI. Default is `enable`.

snat-route-change {enable | disable}

Enable/disable static NAT route change. Default is `disable`.

special-file-23-support {enable | disable}

Enable/disable IPS detection of HIBUN format files when using Data Leak Protection. Default is `disable`.

sslvpn-cipher-hardware-acceleration {enable | disable}

Enable/disable SSL VPN hardware acceleration.

sslvpn-kxp-hardware-acceleration {enable | disable}

Enable/disable SSL VPN KXP hardware acceleration.

sslvpn-max-worker-count <count_int>

Specify the maximum number of SSL VPN processes. The upper limit for setting this value is the number of CPUs and depends on the model.

sslvpn-plugin-version-check {enable | disable}

Enable/disable checking browser's plugin version. Default is `enable`.

strict-dirty-session-check {enable | disable}

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. Default is `enable`.

strong-crypto {enable | disable}

Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). In addition, some low-crypto options are not available. Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption. Default is `disable`. Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). In addition, some low-crypto options are not available. Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption. Default is `disable`.

switch-controller {enable | disable}

Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself. Default is `disable`.

switch-controller-reserved-network <ipv4mask>

Enable reserved network subnet for controlled switches. This is available when the switch controller is enabled. Default: 169.254.0.0 255.255.0.0

syncinterval <ntpsync_minutes>

Specify how often, in minutes, the FortiGate unit should synchronize its time with the Network Time Protocol (NTP) server. Range: 1 - 1440 minutes (1 day). Setting to 0 disables time synchronization. Default is 0.

sys-perf-log-interval <int>

Set the time in minutes between updates of performance statistics logging. Range: 1 - 15 minutes. 0 disables performance logging. Default is 5.

tcp-halfclose-timer <seconds>

Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. Range: 1 - 86400 seconds (1 day). Default is 120.

tcp-halfopen-timer <seconds>

Enter how many 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. Range: 1 - 86400 seconds (1 day). Default is 10.

tcp-option {enable | disable}

Enable SACK, timestamp and MSS TCP options. For normal operation, `tcp-option` should be enabled. Disable for performance testing or, in rare cases, where it impairs performance. Default is `enable`.

tcp-timewait-timer <seconds_int>

Set the length of the TCP TIME-WAIT state in seconds. As described in [RFC 793](#), the "TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request". Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. Range: 0 - 300 seconds. Default is 1.

timezone <timezone_number>

The 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. Default is 00, which is equivalent to GMT +12.

tp-mc-skip-policy {enable | disable}

Enable to allow skipping of the policy check, and to enable multicast traffic through. Default is `disable`. Multicasting (also called IP multicasting) is a technique for one-to-many and many-to-many real-time communication over an IP infrastructure in a network. Multicast uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. can be used to send data to many receivers simultaneously while conserving bandwidth and reducing network traffic. Multicasting can be used for one-way delivery of media streams to multiple receivers and for one-way data transmission for news feeds, financial information, and so on.

traffic-priority {tos | dscp}

Select Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping. Default is `tos`. For more information, see the Handbook's discussion of [ToS and DSCP traffic mapping](#).

traffic-priority-level {low | medium | high}

Select the default system-wide level of priority for traffic prioritization. This determines the priority of traffic for scheduling, typically set on a per service type level. For more information, see `system tos-based-priority` or `system dscp-based-priority` or the [Traffic Shaping](#) chapter in the Handbook. Default is `medium`.

two-factor-email-expiry <seconds_int>

Set the timeout period for email-based two-factor authentication. Two-factor email authentication sends a randomly generated six-digit numeric code to a specified email address. The recipient must enter that code when prompted and that code is only valid for the time period set by this command. Range: 30 - 300 seconds (5 minutes). Default is 60.

two-factor-fac-expiry <seconds_int>

Set the timeout period for FortiAuthenticator token authentication. A FortiAuthenticator provides RADIUS, LDAP and 802.1X wireless authentication, certificate management, and Fortinet Single Sign-on (FSSO). FortiAuthenticator is compatible with FortiToken to provide two-factor authentication with multiple FortiGates and third party devices. Range: 10 - 3600 seconds (1 hour). Default is 60.

two-factor-ftk-expiry <seconds_int>

Set the timeout period for FortiToken authentication. Range: 60 - 600 seconds (10 minutes). Default is 60. FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes at the end of the timeout period set by this command.

two-factor-ftm-expiry <hours_int>

Set the timeout period for FortiToken Mobile provision. Range: 1 - 168 hours (7 days). Default is 72. FortiToken Mobile performs much the same function as the FortiToken except the physical device is replaced by a mobile phone application and the timeout period is set in hours, not seconds.

two-factor-sms-expiry <seconds_int>

Set the timeout period for SMS-based two-factor authentication. Range 30 - 300 seconds. Default is 60. SMS two-factor authentication sends the token code in an SMS text message to the mobile device indicated when this user attempts to logon. This token code is valid only for the time period set by this command. SMS two-factor authentication has the benefit of not requiring email service before logging on. A potential issue is if the mobile service provider does not send the SMS text message before the life of the token expires.

udp-idle-timer <seconds>

Enter the number of seconds before an idle UDP connection times out. This command can be useful in managing unit CPU and memory resources. Range: 1 - 86400 seconds (1 day). Default is 180.

user-server-cert <cert_name>

Select the certificate to use for https user authentication. Default setting is `Fortinet_Factory`, if available, otherwise `self-sign`.

vdom-admin {enable | disable}

Enable/disable configuration of multiple virtual domains. Default is disable.

vip-arp-range {restricted |unlimited}

`vip-arp-range` controls the number of Address Resolution Protocol (ARP) packets the FortiGate unit sends for a Virtual IP (VIP) address range. Default is `restricted`.

- `restricted`: the FortiGate unit sends ARP packets for only the first 8192 addresses in a VIP range.
- `unlimited`: the FortiGate unit sends ARP packets for every address in the VIP range.

virtual-server-count <integer>

Enter the number of virtual server processes to create. The maximum is the number of CPU cores. This is not available on single-core CPUs.

virtual-server-hardware-acceleration {enable | disable}

Enable/disable virtual server hardware acceleration. Default is `enable`.

wad-worker-count <int>

Set the number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy and web caching is handled by half of the CPU cores in a FortiGate unit. For example, if your FortiGate unit has 4 CPU cores, by default two will be used for WAN optimization, explicit proxy and web caching. You can use the `wad-worker-count` command to change the number of CPU cores that are used. Range: 1 to the number of CPU cores.

wifi-ca-certificate <ca_cert-name>

Select the CA certificate that verifies the WiFi certificate.

wifi-certificate <cert-name>

Select the certificate to use for WiFi authentication.

wimax-4g-usb {enable | disable}

Enable/disable access to a Worldwide Interoperability for Microwave Access (WiMAX) 4G USB device. FortiGate units support the use of wireless, 3G and 4G modems connected using the USB port or, if available, the express card slot. Modem access provides either primary or secondary (redundant) access to the Internet. For FortiGate units that do not include an internal modem (those units with an "M" designation), the modem interface will not appear in the web-based manager until enabled in the CLI. Default is `disable`.

wireless-controller {enable | disable}

Enable/disable the wireless (WiFi) daemon. Default is `enable`.

wireless-controller-port <port_int>

Select the 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. Range: 1024 - 49150. Default is 5246.

system gre-tunnel

Introduction.

```
config system gre-tunnel
  edit { name }
  # Configure GRE tunnel.
  set name { string } Tunnel name. size[15]
  set interface { string } Interface name. size[15] - datasource(s): system.interface.name
  set remote-gw { ipv4 address } IP address of the remote gateway.
  set local-gw { ipv4 address any } IP address of the local gateway.
  set sequence-number-transmission { disable | enable } Enable/disable including of sequence numbers in transmitted GRE packets.
  set sequence-number-reception { disable | enable } Enable/disable validating sequence numbers in received GRE packets.
  set checksum-transmission { disable | enable } Enable/disable including checksums in transmitted GRE packets.
  set checksum-reception { disable | enable } Enable/disable validating checksums in received GRE packets.
  set key-outbound { integer } Include this key in transmitted GRE packets (0 - 4294967295). range[0-4294967295]
  set key-inbound { integer } Require received GRE packets contain this key (0 - 4294967295). range[0-4294967295]
  set dscp-copying { disable | enable } Enable/disable DSCP copying.
  set keepalive-interval { integer } Keepalive message interval (0 - 32767, 0 = disabled). range[0-32767]
  set keepalive-failtimes { integer } Number of consecutive unreturned keepalive messages before a GRE connection is considered down (1 -
255). range[1-255]
  next
end
```

system ha

Enable and configure FortiGate FGCP high availability (HA) and virtual clustering. Some of these options are also used for FGSP HA and content clustering.



In FGCP HA mode, most settings are automatically synchronized among cluster units. The following settings are not synchronized:

- override
- priority (including the secondary-vcluster priority)
- ha-mgmt-interface-gateway
- ha-mgmt-interface-gateway6
- cpu-threshold, memory-threshold, http-proxy-threshold, ftp-proxy-threshold, imap-proxy-threshold, nntp-proxy-threshold, pop3-proxy-threshold, smtp-proxy-threshold
- The ha-priority setting of the config system link-monitor command
- The config system interface settings of the FortiGate interface that becomes an HA reserved management interface
- The config system global hostname setting.

CLI Syntax

```
config system ha
  set group-id { integer } Cluster group ID (0 - 255). Must be the same for all members. range[0-255]
  set group-name { string } Cluster group name. Must be the same for all members. size[32]
  set mode { standalone | a-a | a-p } HA mode. Must be the same for all members. FGSP requires standalone.
    standalone Standalone mode.
    a-a Active-active mode.
    a-p Active-passive mode.
  set sync-packet-balance { enable | disable } Enable/disable HA packet distribution to multiple CPUs.
  set password { password_string } Cluster password. Must be the same for all members. size[128]
  set key { password_string } key size[16]
  set hbdev { string } Heartbeat interfaces. Must be the same for all members.
  set session-sync-dev { string } Offload session sync to one or more interfaces to distribute traffic and prevent delays if needed.
  set route-ttl { integer } TTL for primary unit routes (5 - 3600 sec). Increase to maintain active routes during failover. range[5-3600]
  set route-wait { integer } Time to wait before sending new routes to the cluster (0 - 3600 sec). range[0-3600]
  set route-hold { integer } Time to wait between routing table updates to the cluster (0 - 3600 sec). range[0-3600]
```

```

set multicast-ttl { integer } HA multicast TTL on master (5 - 3600 sec). range[5-3600]
set load-balance-all { enable | disable } Enable to load balance TCP sessions. Disable to load balance proxy sessions only.
set sync-config { enable | disable } Enable/disable configuration synchronization.
set encryption { enable | disable } Enable/disable heartbeat message encryption.
set authentication { enable | disable } Enable/disable heartbeat message authentication.
set hb-interval { integer } Time between sending heartbeat packets (1 - 20 (100*ms)). Increase to reduce false positives. range[1-20]
set hb-lost-threshold { integer } Number of lost heartbeats to signal a failure (1 - 60). Increase to reduce false positives. range[1-60]
set hello-holddown { integer } Time to wait before changing from hello to work state (5 - 300 sec). range[5-300]
set gratuitous-arps { enable | disable } Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.
set arps { integer } Number of gratuitous ARPs (1 - 60). Lower to reduce traffic. Higher to reduce failover time. range[1-60]
set arps-interval { integer } Time between gratuitous ARPs (1 - 20 sec). Lower to reduce failover time. Higher to reduce traffic. range[1-20]
set session-pickup { enable | disable } Enable/disable session sync. Only useful in special cases. Enabling can reduce performance.
set session-pickup-connectionless { enable | disable } Enable/disable UDP and ICMP session sync for FGSP.
set session-pickup-expectation { enable | disable } Enable/disable session helper expectation session sync for FGSP.
set session-pickup-nat { enable | disable } Enable/disable NAT session sync for FGSP.
set session-pickup-delay { enable | disable } Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.
set session-sync-daemon-number { integer } For ELBC cluster to 2 members. Increase the number of processes if session rate is high. range[1-15]
set link-failed-signal { enable | disable } Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update
network.
set uninterruptible-upgrade { enable | disable } Enable to upgrade a cluster without blocking network traffic.
set standalone-mgmt-vdom { enable | disable } Enable/disable standalone management VDOM.
set ha-mgmt-status { enable | disable } Enable to reserve interfaces to manage individual cluster units.
config ha-mgmt-interfaces
edit { id }
# Reserve interfaces to manage individual cluster units.
set id { integer } Table ID. range[0-4294967295]
set interface { string } Interface to reserve for HA management. size[15] - datasource(s): system.interface.name
set dst { ipv4 classnet } Default route destination for reserved HA management interface.
set gateway { ipv4 address } Default route gateway for reserved HA management interface.
set gateway6 { ipv6 address } Default IPv6 gateway for reserved HA management interface.
next
set ha-eth-type { string } HA heartbeat packet Ethertype (4-digit hex). size[4]
set hc-eth-type { string } Transparent mode HA heartbeat packet Ethertype (4-digit hex). size[4]
set l2ep-eth-type { string } Telnet session HA heartbeat packet Ethertype (4-digit hex). size[4]
set ha-uptime-diff-margin { integer } Normally you would only reduce this value for failover testing. range[1-65535]
set standalone-config-sync { enable | disable } Enable/disable FGSP configuration synchronization.
set vcluster2 { enable | disable } Enable/disable virtual cluster 2 for virtual clustering.
set vcluster-id { integer } Cluster ID. range[0-255]
set override { enable | disable } Enable and increase the priority of the unit that should always be primary (master).
set priority { integer } Increase the priority to select the primary unit (0 - 255). range[0-255]
set override-wait-time { integer } Delay negotiating if override is enabled (0 - 3600 sec). Reduces how often the cluster negotiates. range[0-
3600]
set schedule { option } Type of A-A load balancing. Use none if you have external load balancers.

```

```

    none                None.
    hub                 Hub.
    leastconnection     Least connection.
    round-robin         Round robin.
    weight-round-robin  Weight round robin.
    random              Random.
    ip                  IP.
    ipport              IP port.
set weight { string }  Weight-round-robin weight for each cluster unit. Syntax { priority } { weight }.
set cpu-threshold { string }  Dynamic weighted load balancing CPU usage weight and high and low thresholds.
set memory-threshold { string }  Dynamic weighted load balancing memory usage weight and high and low thresholds.
set http-proxy-threshold { string }  Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.
set ftp-proxy-threshold { string }  Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.
set imap-proxy-threshold { string }  Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.
set nntp-proxy-threshold { string }  Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.
set pop3-proxy-threshold { string }  Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.
set smtp-proxy-threshold { string }  Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.
set monitor { string }  Interfaces to check for port monitoring (or link failure).
set pingserver-monitor-interface { string }  Interfaces to check for remote IP monitoring.
set pingserver-failover-threshold { integer }  Remote IP monitoring failover threshold (0 - 50). range[0-50]
set pingserver-slave-force-reset { enable | disable }  Enable to force the cluster to negotiate after a remote IP monitoring failover.
set pingserver-flip-timeout { integer }  Time to wait in minutes before renegotiating after a remote IP monitoring failover. range[6-2147483647]
set vdom { string }  VDOMs in virtual cluster 1.
    set vcluster-id { integer }  Cluster ID. range[0-255]
    set override { enable | disable }  Enable and increase the priority of the unit that should always be primary (master).
    set priority { integer }  Increase the priority to select the primary unit (0 - 255). range[0-255]
    set override-wait-time { integer }  Delay negotiating if override is enabled (0 - 3600 sec). Reduces how often the cluster negotiates. range
[0-3600]
set monitor { string }  Interfaces to check for port monitoring (or link failure).
set pingserver-monitor-interface { string }  Interfaces to check for remote IP monitoring.
set pingserver-failover-threshold { integer }  Remote IP monitoring failover threshold (0 - 50). range[0-50]
set pingserver-slave-force-reset { enable | disable }  Enable to force the cluster to negotiate after a remote IP monitoring failover.
set vdom { string }  VDOMs in virtual cluster 2.
set ha-direct { enable | disable }  Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer,
FortiManager and FortiSandbox.
set memory-compatible-mode { enable | disable }  Enable/disable memory compatible mode.
end

```

Supplemental Information

The following section is for those commands that require further explanation.

group-id <id>

The HA group ID, same for all members, from 0 to 255. The group ID identifies individual clusters on the network because the group ID affects the cluster virtual MAC address. All cluster members must have the same group ID. If you have more than two clusters on the same network they must have different Group IDs.

group-name <name>

The HA group name, same for all members. Max 32 characters. The HA group name identifies the cluster. All cluster members must have the same group name. Can be blank if mode is `standalone`.

mode {standalone | a-a | a-p}

The HA mode.

- `standalone` to disable HA. The mode required for FGSP.
- `a-a` to create an Active-Active cluster.
- `a-p` to create an Active-Passive cluster.

All members of an HA cluster must be set to the same HA mode.

password <password>

The HA cluster password, must be the same for all cluster units. The maximum password length is 15 characters.

hbdev <interface-name> <priority> [<interface-name> <priority>]...

Select the FortiGate interfaces to be heartbeat interfaces and set the heartbeat priority for each interface. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface that with the lowest hash map order value processes all heartbeat traffic.

By default two interfaces are configured to be heartbeat interfaces and the priority for both these interfaces is set to 50. The heartbeat interface priority range is 0 to 512.

You can select up to 8 heartbeat interfaces. This limit only applies to FortiGate units with more than 8 physical interfaces.

You can use the `append` command to add more entries. The default depends on the FortiGate model.

session-sync-dev <interface>

Select one or more FortiGate interfaces to use for synchronizing sessions as required for session pickup. Normally session synchronization occurs over the HA heartbeat link. Using this HA option means only the selected interfaces are used for session synchronization and not the HA heartbeat link. If you select more than one interface, session synchronization traffic is load balanced among the selected interfaces.

Moving session synchronization from the HA heartbeat interface reduces the bandwidth required for HA heartbeat traffic and may improve the efficiency and performance of the cluster, especially if the cluster is synchronizing a large number of sessions. Load balancing session synchronization among multiple interfaces can further improve performance and efficiency if the cluster is synchronizing a large number of sessions.

Session synchronization packets use Ethertype 0x8892. The interfaces to use for session synchronization must be connected together either directly using the appropriate cable (possible if there are only two units in the cluster) or using switches. If one of the interfaces becomes disconnected the cluster uses the remaining interfaces for session synchronization. If all of the session synchronization interfaces become disconnected, session synchronization reverts back to using the HA heartbeat link. All session synchronization traffic is between the primary unit and each subordinate unit.

Since large amounts of session synchronization traffic can increase network congestion, it is recommended that you keep this traffic off of your network by using dedicated connections for it.

route-ttl <ttl>

Control how long routes remain in a cluster unit's routing table. The time to live range is 5 to 3600 seconds (3600 seconds is one hour). The default time to live is 10 seconds.

The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. To maintain communication sessions after a cluster unit becomes a primary unit, routes remain active in the routing table for the route time to live while the new primary unit acquires new routes.

By default, `route-ttl` is set to 10 which may mean that only a few routes will remain in the routing table after a failover. Normally keeping `route-ttl` to 10 or reducing the value to 5 is acceptable because acquiring new routes usually occurs very quickly, especially if graceful restart is enabled, so only a minor delay is caused by acquiring new routes.

If the primary unit needs to acquire a very large number of routes, or if for other reasons there is a delay in acquiring all routes, the primary unit may not be able to maintain all communication sessions.

You can increase the route time to live if you find that communication sessions are lost after a failover so that the primary unit can use synchronized routes that are already in the routing table, instead of waiting to acquire new routes.

route-wait <wait>

The amount of time in seconds that the primary unit waits after receiving routing updates before sending the updates to the subordinate units. For quick routing table updates to occur, set `route-wait` to a relatively short time so that the primary unit does not hold routing table changes for too long before updating the subordinate units.

The `route-wait` range is 0 to 3600 seconds. The default `route-wait` is 0 seconds. Normally, because the is 0 seconds.

Normally, because the `route-wait` time is 0 seconds the primary unit sends routing table updates to the subordinate units every time its routing table changes.

Once a routing table update is sent, the primary unit waits the `route-hold` time before sending the next update.

Usually routing table updates are periodic and sporadic. Subordinate units should receive these changes as soon as possible so `route-wait` is set to 0 seconds. `route-hold` can be set to a relatively long time because normally the next route update would not occur for a while.

In some cases, routing table updates can occur in bursts. A large burst of routing table updates can occur if a router or a link on a network fails or changes. When a burst of routing table updates occurs, there is a potential that the primary unit could flood the subordinate units with routing table updates. Flooding routing table updates can affect cluster performance if a great deal of routing information is synchronized between cluster units. Setting `route-wait` to a longer time reduces the frequency of additional updates are and prevents flooding of routing table updates from occurring.

route-hold <hold>

The amount of time in seconds that the primary unit waits between sending routing table updates to subordinate units. The route hold range is 0 to 3600 seconds. The default route hold time is 10 seconds.

To avoid flooding routing table updates to subordinate units, set `route-hold` to a relatively long time to prevent subsequent updates from occurring too quickly. Flooding routing table updates can affect cluster performance if a great deal of routing information is synchronized between cluster units. Increasing the time between updates means that this data exchange will not have to happen so often.

The `route-hold` time should be coordinated with the `route-wait` time.

sync-config {disable | enable}

Enable or disable automatic synchronization configuration changes to all cluster units.

encryption {disable | enable}

Enable or disable HA heartbeat message encryption using AES-128 for encryption and SHA1 for authentication. Disabled by default.

authentication {disable | enable}

Enable or disable HA heartbeat message authentication using SHA1. Disabled by default.

hb-interval <interval>

The time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100*milliseconds). The default is 2.

A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms (5 * 100ms = 500ms).

HA heartbeat packets consume more bandwidth if the heartbeat interval is short. But if the heartbeat interval is very long, the cluster is not as sensitive to topology and other network changes.

The heartbeat interval combines with the lost heartbeat threshold to set how long a cluster unit waits before assuming that another cluster unit has failed and is no longer sending heartbeat packets. By default, if a cluster unit does not receive a heartbeat packet from a cluster unit for $6 * 200 = 1200$ milliseconds or 1.2 seconds the cluster unit assumes that the other cluster unit has failed.

You can increase both the heartbeat interval and the lost heartbeat threshold to reduce false positives. For example, increasing the heartbeat interval to 20 and the lost heartbeat threshold to 30 means a failure will be assumed if no heartbeat packets are received after $30 * 2000$ milliseconds = 60,000 milliseconds, or 60 seconds.

hb-lost-threshold <threshold>

The number of consecutive heartbeat packets that are not received from another cluster unit before assuming that the cluster unit has failed. The default value is 6, meaning that if the 6 heartbeat packets are not received from a cluster unit then that cluster unit is considered to have failed. The range is 1 to 60 packets.

If the primary unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed.

If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit.

The lower the `hb-lost-threshold` the faster a cluster responds when a unit fails. However, sometimes heartbeat packets may not be sent because a cluster unit is very busy. This can lead to a false positive failure detection. To reduce these false positives you can increase the `hb-lost-threshold`.

hello-holddown <timer>

The number of seconds that a cluster unit waits before changing from the hello state to the work state. The default is 20 seconds and the range is 5 to 300 seconds.

The hello state hold-down time is the number of seconds that a cluster unit waits before changing from hello state to work state. After a failure or when starting up, cluster units operate in the hello state to send and receive heartbeat packets so that all the cluster units can find each other and form a cluster. A cluster unit should change from the hello state to work state after it finds all of the other FortiGate units to form a cluster with. If for some reason all cluster units cannot find each other during the hello state then some cluster units may be joining the cluster after it has formed. This can cause disruptions to the cluster and affect how it operates.

One reason for a delay in all of the cluster units joining the cluster could be the cluster units are located at different sites or if for some other reason communication is delayed between the heartbeat interfaces.

If cluster units are joining your cluster after it has started up or if it takes a while for units to join the cluster you can increase the time that the cluster units wait in the hello state.

gratuitous-arps {disable | enable}

Enable or disable sending gratuitous ARP packets from a new master unit. Enabled by default.

In most cases you would want to send gratuitous ARP packets because it's a reliable way for the cluster to notify the network to send traffic to the new primary unit. However, in some cases, sending gratuitous ARP packets may be less optimal. For example, if you have a cluster of FortiGate units in Transparent mode, after a failover the new primary unit will send gratuitous ARP packets to all of the addresses in its Forwarding Database (FDB). If the FDB has a large number of addresses it may take extra time to send all the packets and the sudden burst of traffic could disrupt the network.

If you choose to disable sending gratuitous ARP packets you must first enable the `link-failed-signal` setting. The cluster must have some way of informing attached network devices that a failover has occurred.

arps <number>

The number of times that the primary unit sends gratuitous ARP packets. Gratuitous ARP packets are sent when a cluster unit becomes a primary unit (this can occur when the cluster is starting up or after a failover). The default is 5 packets, the range is 1 to 60.

Usually you would not change the default setting of 5. In some cases, however, you might want to reduce the number of gratuitous ARP packets. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending a higher number of gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully, you could reduce the number of gratuitous ARP packets that are sent to reduce the amount of traffic produced after a failover.

If failover is taking longer than expected, you may be able to reduce the failover time by increasing the number of gratuitous ARP packets sent.

arps-interval <interval>

The number of seconds to wait between sending gratuitous ARP packets. When a cluster unit becomes a primary unit (this occurs when the cluster is starting up or after a failover) the primary unit sends gratuitous ARP packets immediately to inform connected network equipment of the IP address and MAC address of the primary unit. The default is 8 seconds, the range is 1 to 20 seconds.

Normally you would not need to change the time interval. However, you could decrease the time to be able send more packets in less time if your cluster takes a long time to failover.

There may also be a number of reasons to set the interval higher. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully you could increase the interval to reduce the amount of traffic produced after a failover.

session-pickup {disable | enable}

Enable or disable session pickup. Disabled by default.

Enable session-pickup so that if the primary unit fails, all sessions are picked up by the new primary unit. If you enable session pickup the subordinate units maintain session tables that match the primary unit session table. If the primary unit fails, the new primary unit can maintain most active communication sessions.

If you do not enable session pickup the subordinate units do not maintain session tables. If the primary unit fails all sessions are interrupted and must be restarted when the new primary unit is operating.

Many protocols can successfully restart sessions with little, if any, loss of data. For example, after a failover, users browsing the web can just refresh their browsers to resume browsing. Since most HTTP sessions are very short, in most cases they will not even notice an interruption unless they are downloading large files. Users downloading a large file may have to restart their download after a failover.

Other protocols may experience data loss and some protocols may require sessions to be manually restarted. For example, a user downloading files with FTP may have to either restart downloads or restart their FTP client.

session-pickup-connectionless {disable | enable}

Enable or disable session synchronization for connectionless (UDP and ICMP) sessions when `mode` is set to `a-a` or `a-p`. When `mode` is standalone, session pickup applies to FGSP cluster TCP session synchronization only. This is available if session-pickup is enabled but by default it is disabled.

session-pickup-expectation {disable | enable}

Enable or disable session synchronization for expectation sessions in an FGSP cluster. This is available if session-pickup is enabled and mode is standalone and is disabled by default.

FortiOS session helpers keep track of the communication of Layer-7 protocols such as FTP and SIP that have control sessions and expectation sessions. Usually the control sessions establish the link between server and client and negotiate the ports and protocols that will be used for data communications. The session helpers then create expectation sessions through the FortiGate for the ports and protocols negotiated by the control session.

The expectation sessions are usually the sessions that actually communicate data. For FTP, the expectation sessions transmit files being uploaded or downloaded. For SIP, the expectation sessions transmit voice and video data. Expectation sessions usually have a timeout value of 30 seconds. If the communication from the server is not initiated within 30 seconds the expectation session times out and traffic will be denied.

session-pickup-nat {disable | enable}

Enable or disable session synchronization for NAT sessions in an FGSP cluster. This is available if session-pickup is enabled and mode is standalone and is disabled by default.

session-pickup-delay {disable | enable}

Enable or disable synchronizing sessions only if they remain active for more than 30 seconds. This option improves performance when session-pickup is enabled by reducing the number of sessions that are synchronized.

session-sync-daemon-number <number>

The number of processes used by the HA session sync daemon. Increase the number of processes to handle session packets sent from the kernel efficiently when the session rate is high. Intended for ELBC clusters, this feature only works for clusters with two members. The default is 1, the range 1 to 15.

link-failed-signal {disable | enable}

Enable or disable shutting down all interfaces (except for heartbeat device interfaces) of a cluster unit with a failed monitored interface for one second after a failover occurs. Enable this option if the switch the cluster is connected to does not update its MAC forwarding tables after a failover caused by a link failure. Disabled by default.

If you choose to disable sending gratuitous ARP packets (by setting `gratuitous-arps` to `disable`) you must first enable `link-failed-signal`. The cluster must have some way of informing attached network devices that a failover has occurred.

uninterruptible-upgrade {disable | enable}

Enable or disable upgrading the cluster without interrupting cluster traffic processing. Enabled by default.

If `uninterruptible-upgrade` is enabled, traffic processing is not interrupted during a normal firmware upgrade. This process can take some time and may reduce the capacity of the cluster for a short time. If is enabled, traffic processing is not interrupted during a normal firmware upgrade. This process can take some time and may reduce the capacity of the cluster for a short time.

If `uninterruptible-upgrade` is disabled, traffic processing is interrupted during a normal firmware upgrade (similar to upgrading the firmware operating on a standalone FortiGate unit).

ha-mgmt-status {enable | disable}

Enable or disable the HA reserved management interface feature. Disabled by default.

ha-mgmt-interface <interface_name>

The FortiGate interface to be the reserved HA management interface. You can configure the IP address and other settings for this interface using the `config system interface` command. When you enable the reserved management interface feature the configuration of the reserved management interface is not synchronized by the FGCP.

ha-mgmt-interface-gateway <gateway_IP>

The default route for the reserved HA management interface (IPv4). This setting is not synchronized by the FGCP.

ha-mgmt-interface-gateway6 <gateway_IP>

The default route for the reserved HA management interface (IPv6). This setting is not synchronized by the FGCP.

ha-eth-type <type>

The Ethertype used by HA heartbeat packets for NAT/Route mode clusters. <type> is a 4-digit number. Default is 8890.

hc-eth-type <type>

The Ethertype used by HA heartbeat packets for Transparent mode clusters. <type> is a 4-digit number. Default is 8891.

l2ep-eth-type <type>

The Ethertype used by HA telnet sessions between cluster units over the HA link. <type> is a 4-digit number. Default is 8893.

ha-uptime-diff-margin <margin>

The cluster age difference margin (grace period). This margin is the age difference ignored by the cluster when selecting a primary unit based on age. Normally the default value of 300 seconds (5 minutes) should not be changed. However, for demo purposes you can use this option to lower the difference margin. The range is 1 to 65535 seconds.

You may want to reduce the margin if during failover testing you don't want to wait the default age difference margin of 5 minutes. You may also want to reduce the margin to allow uninterruptible upgrades to work.

You may want to increase the age margin if cluster unit startup time differences are larger than 5 minutes.

During a cluster firmware upgrade with `uninterruptible-upgrade` enabled (the default configuration) the cluster should not select a new primary unit after the firmware of all cluster units has been updated. But since the age difference of the cluster units is most likely less than 300 seconds, age is not used to affect primary unit selection and the cluster may select a new primary unit.

During failover testing where cluster units are failed over repeatedly the age difference between the cluster units will most likely be less than 5 minutes. During normal operation, if a failover occurs, when the failed unit rejoins the cluster its age will be very different from the age of the still operating cluster units so the cluster will not select a new primary unit. However, if a unit fails and is restored in a very short time the age difference may be less than 5 minutes. As a result the cluster may select a new primary unit during some failover testing scenarios.

vcluster2 {disable | enable}

Enable or disable virtual cluster 2 (also called secondary-vcluster).

When multiple VDOMs are enabled, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use `config secondary-vcluster` to configure virtual cluster 2.

Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.

Enabling virtual cluster 2 enables `override` for virtual cluster 1 and virtual cluster 2.

vcluster-id

Indicates the virtual cluster you are configuring. You can't change this setting. You can use the `config secondary-vcluster` command to edit vcluster 2.

standalone-config-sync {disable | enable}

Synchronize the configuration of the FortiGate unit in an FGSP cluster. This is available if `session-pickup` is enabled and `mode` is `standalone`. Disabled by default.

override {disable | enable}

Enable or disable forcing the cluster to renegotiate and select a new primary unit every time a cluster unit leaves or joins a cluster, changes status within a cluster, or every time the HA configuration of a cluster unit changes.

Disabled by default. Automatically enabled when you enable virtual cluster 2. This setting is not synchronized to other cluster units.

In most cases you should keep `override` disabled to reduce how often the cluster negotiates. Frequent negotiations may cause frequent traffic interruptions. However, if you want to make sure that the same cluster unit always operates as the primary unit and if you are less concerned about frequent cluster negotiation you can set its device priority higher than other cluster units and enable `override`.

priority <priority>

The device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the cluster unit with the highest device priority becomes the primary unit. The device priority range is 0 to 255. The default is 128. This setting is not synchronized to other cluster units.

override-wait-time <seconds>

Delay renegotiating when `override` is enabled and HA is enabled or the cluster mode is changed or after a cluster unit reboots. You can add a time to prevent negotiation during transitions and configuration changes. Range 0 to 3600 seconds.

schedule {hub | ip | ipport | leastconnection | none | random | round-robin | weight-round-robin}

The cluster's active-active load balancing schedule.

- `hub` load balancing if the cluster interfaces are connected to hubs. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet.
- `ip` load balancing according to IP address.
- `ipport` load balancing according to IP address and port.
- `leastconnection` least connection load balancing.
- `none` no load balancing. Use when the cluster interfaces are connected to load balancing switches.

- `random` random load balancing.
- `round-robin` round robin load balancing. If the cluster units are connected using switches, use round-robin to distribute traffic to the next available cluster unit.
- `weight-round-robin` weighted round robin load balancing. Similar to `round robin`, but you can assign weighted values to each of the units in the cluster.

slave-switch-standby {disable | enable}

Enable to force a subordinate FortiSwitch-5203B or FortiController-5902D into standby mode even though its weight is non-zero. This is a content clustering option and is disabled by default.

minimum-worker-threshold <threshold>

Available on FortiSwitch-5203Bs or FortiController-5902Ds only in inter-chassis content-cluster mode. In inter-chassis mode the system considers the number of operating workers in a chassis when electing the primary chassis. A chassis that has less than the `minimum-worker-threshold` of workers operating is ranked lower than a chassis that meets or exceeds the `minimum-worker-threshold`. The default value of 1 effectively disables the threshold. The range is 1 to 11.

monitor <interface-name> [<interface-name>...]

Enable or disable port monitoring for link failure. Port monitoring (also called interface monitoring) monitors FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks.

Enter the names of the interfaces to monitor. Use a space to separate each interface name. Use append to add an interface to the list. If there are no monitored interfaces then port monitoring is disabled.

You can monitor physical interfaces, redundant interfaces, and 802.3ad aggregated interfaces but not VLAN interfaces, IPSec VPN interfaces, or switch interfaces.

You can monitor up to 64 interfaces. In a multiple VDOM configuration you can monitor up to 64 interfaces per virtual cluster.

pingserver-monitor-interface <interface-name> [<interface-name>...]

Enable HA remote IP monitoring by specifying the FortiGate unit interfaces that will be used to monitor remote IP addresses. You can configure remote IP monitoring for all types of interfaces including physical interfaces, VLAN interfaces, redundant interfaces and aggregate interfaces.

Use a space to separate each interface name. Use append to add an interface to the list.

pingserver-failover-threshold <threshold>

The HA remote IP monitoring failover threshold. The failover threshold range is 0 to 50. Setting the failover threshold to 0 (the default) means that if any ping server added to the HA remote IP monitoring configuration fails an HA failover will occur.

Set the priority for each remote IP monitoring ping server using the `ha-priority` option of the `config system link-monitor` command. Increase the priority to require more remote links to fail before a failover occurs.

pingserver-slave-force-reset {disable | enable}

In a remote IP monitoring configuration, if you also want the same cluster unit to always be the primary unit you can set its device priority higher and enable override. With this configuration, when a remote IP monitoring failover occurs, after the flip timeout expires another failover will occur (because override is enabled) and the unit with override enabled becomes the primary unit again. So the cluster automatically returns to normal operation.

The primary unit starts remote IP monitoring again. If the remote link is restored the cluster continues to operate normally. If, however, the remote link is still down, remote link failover causes the cluster to failover again. This will repeat each time the flip timeout expires until the failed remote link is restored.

You can use the `pingserver-slave-force-reset` option to control this behavior. By default this option is enabled and the behavior described above occurs. The overall behavior is that when the remote link is restored the cluster automatically returns to normal operation after the flip timeout.

If you disable `pingserver-slave-force-reset` after the initial remote IP monitoring failover nothing will happen after the flip timeout (as long as the new primary unit doesn't experience some kind of failover). The result is that repeated failovers no longer happen. But it also means that the original primary unit will remain the subordinate unit and will not resume operating as the primary unit.

pingserver-flip-timeout <timeout>

The HA remote IP monitoring flip timeout in minutes. If HA remote IP monitoring fails on all cluster units because none of the cluster units can connect to the monitored IP addresses, the flip timeout stops a failover from occurring until the timer runs out. The range is 6 to 2147483647 minutes. The default is 60 minutes.

The flip timeout reduces the frequency of failovers if, after a failover, HA remote IP monitoring on the new primary unit also causes a failover. This can happen if the new primary unit cannot connect to one or more of the monitored remote IP addresses. The result could be that until you fix the network problem that blocks connections to the remote IP addresses, the cluster will experience repeated failovers. You can control how often the failovers occur by setting the flip timeout.

The flip timeout stops HA remote IP monitoring from causing a failover until the primary unit has been operating for the duration of the flip timeout. If you set the flip timeout to a relatively high number of minutes you can find and repair the network problem that prevented the cluster from connecting to the remote IP address without the cluster experiencing very many failovers. Even if it takes a while to detect the problem, repeated failovers at relatively long time intervals do not usually disrupt network traffic.

The flip timeout also causes the cluster to renegotiate when it expires unless you have disabled `pingserver-slave-force-reset`.

vdom <vdom-name> [<vdom-name>...]

Add virtual domains to a virtual cluster. By default all VDOMs are added to virtual cluster 1. Adding a virtual domain to a virtual cluster removes it from the other virtual cluster. You add VDOMs to virtual cluster 1 using the following syntax:

```
config system ha
    set vdom root vdom1
end
```

You add VDOMs to virtual cluster 2 using the following syntax:

```
config system ha
    set secondary-vcluster enable
    config vcluster2
        set vdom root vdom1
    end
end
```

ha-direct {disable | enable}

Enable to use the HA management interface for management access for sending log messages to FortiAnalyzer, or remote syslog servers, and for SNMP, access to remote authentication servers (for example, RADIUS, LDAP), FortiManager, FortiSandbox and so on.

Disabled by default. Only appears if `ha-mgmt-status` is enabled.

load-balance-all {disable | enable}

By default, active-active HA load balancing distributes proxy-based security profile processing to all cluster units. Proxy-based security profile processing is CPU and memory-intensive, so FGCP load balancing may result in higher throughput because resource-intensive processing is distributed among all cluster units.

Proxy-based security profile processing that is load balanced includes proxy-based virus scanning, proxy-based web filtering, proxy-based email filtering, and proxy-based data leak prevention (DLP) of HTTP, FTP, IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS, IM, and NNTP, sessions accepted by security policies. Other features enabled in security policies such as Endpoint security, traffic shaping and authentication have no effect on active-active load balancing.

You can enable `load-balance-all` to have the primary unit load balance all TCP sessions. Load balancing TCP sessions increases overhead and may actually reduce performance so it is disabled by default.

load-balance-udp {disable | enable}

Enable or disable load balancing UDP proxy-based security profile sessions. Load balancing UDP sessions increases overhead so it is also disabled by default.

This content clustering option is available for the FortiSwitch-5203B and FortiController-5902D.

weight {0 | 1 | 2 | 3} <weight>

The weighted round robin load balancing weight to assign to each unit in an active-active cluster. The weight is set according to the priority of the unit in the cluster. An FGCP cluster can include up to four FortiGates (numbered 0 to 3) so you can set up to 4 weights. The default weights mean that the four possible units in the cluster all have the same weight of 40. The weight range is 0 to 255. Increase the weight to increase the number of connections processed by the FortiGate with that priority.

Weights are assigned to individual FortiGates according to their priority in the cluster. The priorities are assigned when the cluster negotiates and can change every time the cluster re-negotiates.

You enter the weight for each FortiGate separately. For example, if you have a cluster of three FortiGate units you can set the weights for the units as follows:

```
set weight 0 5
set weight 1 10
set weight 2 15
```

cpu-threshold <weight> <low> <high>

Dynamic weighted load balancing by CPU usage. When enabled fewer sessions will be load balanced to the cluster unit when its CPU usage reaches the high watermark.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

memory-threshold <weight> <low> <high>

Dynamic weighted load balancing by memory usage. When enabled fewer sessions will be load balanced to the cluster unit when its memory usage reaches the high watermark.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

http-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of HTTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

imap-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of IMAP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

nntp-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of NNTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

pop3-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of POP3 proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

smtp-proxy-threshold <weight> <low> <high>

Dynamic weighted load balancing by the number of SMTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark is reached.

This option is available when `mode` is `a-a` and `schedule` is `weight-round-robin`. Default low and high watermarks of 0 disable the feature. The default weight is 5.

This setting is not synchronized by the FGCP so you can set separate weights for each cluster unit.

config secondary-vcluster

Configure virtual cluster 2. You must first enable `vcluster2`. Use the following syntax.

```
config secondary-vcluster
  set vcluster-id 2
  set override {disable | enable}
  set priority <priority>
  set override-wait-time <time>
  {set | append} monitor <interface-name> [<interface-name>...]
  {set | append} pingserver-monitor-interface <interface-name> [<interface-name>...]
  set pingserver-failover-threshold <threshold>
  set pingserver-slave-force-reset {disable | enable}
  {set | append} vdom <vdom-name> [<vdom-name>...]
end
```

system ha-monitor

If the FortiGates in a cluster have VLAN interfaces, you can use this command to monitor all VLAN interfaces and write a log message if one of the VLAN interfaces is found to be down. Once configured, this feature works by verifying that the primary unit can connect to the subordinate unit over each VLAN. This verifies that the switch that the VLAN interfaces are connected to is configured correctly for each VLAN. If the primary unit cannot connect to the subordinate unit over one of the configured VLANs the primary unit writes a link monitor log message indicating that the named VLAN went down (log message id 20099).

```
config system ha-monitor
    set monitor-vlan { enable | disable }  Enable/disable monitor VLAN interfaces.
    set vlan-hb-interval { integer }  Configure heartbeat interval (seconds). range[1-30]
    set vlan-hb-lost-threshold { integer }  VLAN lost heartbeat threshold (1 - 60). range[1-60]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

monitor-vlan {enable | disable}

Enable monitor VLANs. Disabled by default

vlan-hb-interval <integer>

The time between sending VLAN heartbeat packets over the VLAN. The VLAN heartbeat range is 1 to 30 seconds. The default is 5 seconds.

vlan-hb-lost-threshold <integer>

The number of consecutive VLAN heartbeat packets that are not successfully received across the VLAN before assuming that the VLAN is down. The default value is 3, meaning that if 3 heartbeat packets sent over the VLAN are not received then the VLAN is considered to be down. The range is 1 to 60 packets. A VLAN heartbeat interval of 5 means the time between heartbeat packets is five seconds. A VLAN heartbeat threshold of 3 means it takes $5 \times 3 = 15$ seconds to detect that a VLAN is down.

system interface

Configure interface settings.

```
config system interface
  edit { name }
  # Configure interfaces.
  set name { string } Name. size[15]
  set vdom { string } Interface is in this virtual domain (VDM). size[31] - datasource(s): system.vdom.name
  set cli-conn-status { integer } CLI connection status. range[0-4294967295]
  set fortilink { enable | disable } Enable FortiLink to dedicate this interface to manage other Fortinet devices.
  set mode { static | dhcp | pppoe } Addressing mode (static, DHCP, PPPoE).
    static Static setting.
    dhcp External DHCP client mode.
    pppoe External PPPoE mode.
  set distance { integer } Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route. range[1-255]
  set priority { integer } Priority of learned routes. range[0-4294967295]
  set dhcp-relay-service { disable | enable } Enable/disable allowing this interface to act as a DHCP relay.
  set dhcp-relay-ip { string } DHCP relay IP address.
  set dhcp-relay-type { regular | ipsec } DHCP relay type (regular or IPsec).
    regular Regular DHCP relay.
    ipsec DHCP relay for IPsec.
  set management-ip { ipv4 classnet host } High Availability in-band management IP address of this interface.
  set ip { ipv4 classnet host } Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.
  set allowaccess { option } Permitted types of management access to this interface.
    ping PING access.
    https HTTPS access.
    ssh SSH access.
    snmp SNMP access.
    http HTTP access.
    telnet TELNET access.
    fgfm FortiManager access.
    radius-acct RADIUS accounting access.
    probe-response Probe access.
    capwap CAPWAP access.
    ftm FTM access.
  set gwdetect { enable | disable } Enable/disable detect gateway alive for first.
  set ping-serv-status { integer } PING server status. range[0-255]
  set detectserver { string } Gateway's ping server for this IP.
```

```

set detectprotocol { ping | tcp-echo | udp-echo }  Protocols used to detect the server.
    ping      PING.
    tcp-echo  TCP echo.
    udp-echo  UDP echo.
set ha-priority { integer }  HA election priority for the PING server. range[1-50]
set fail-detect { enable | disable }  Enable/disable fail detection features for this interface.
set fail-detect-option { detectserver | link-down }  Options for detecting that this interface has failed.
    detectserver  Use a ping server to determine if the interface has failed.
    link-down     Use port detection to determine if the interface has failed.
set fail-alert-method { link-failed-signal | link-down }  Select link-failed-signal or link-down method to alert about a failed link.
    link-failed-signal  Link-failed-signal.
    link-down           Link-down.
set fail-action-on-extender { soft-restart | hard-restart | reboot }  Action on extender when interface fail .
    soft-restart  Soft-restart-on-extender.
    hard-restart  Hard-restart-on-extender.
    reboot        Reboot-on-extender.
config fail-alert-interfaces
    edit { name }
        # Names of the FortiGate interfaces from which the link failure alert is sent for this interface.
        set name { string }  Names of the physical interfaces belonging to the aggregate or redundant interface. size[64] - datasource(s):
system.interface.name
    next
    set dhcp-client-identifier { string }  DHCP client identifier. size[48]
    set dhcp-renew-time { integer }  DHCP renew time (300 - 604800 sec, 0 means use the renew time provided by the server). range[300-604800]
    set ipunnumbered { ipv4 address }  Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.
    set username { string }  Username of the PPPoE account, provided by your ISP. size[64]
    set pppoe-unnumbered-negotiate { enable | disable }  Enable/disable PPPoE unnumbered negotiation.
    set password { password_string }  PPPoE account's password. size[128]
    set idle-timeout { integer }  PPPoE auto disconnect after idle timeout seconds, 0 means no timeout. range[0-32767]
    set detected-peer-mtu { integer }  MTU of detected peer (0 - 4294967295). range[0-4294967295]
    set disc-retry-timeout { integer }  Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout. range[0-4294967295]
    set padt-retry-timeout { integer }  PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time. range[0-4294967295]
    set service-name { string }  PPPoE service name. size[63]
    set ac-name { string }  PPPoE server name. size[63]
    set lcp-echo-interval { integer }  Time in seconds between PPPoE Link Control Protocol (LCP) echo requests. range[0-32767]
    set lcp-max-echo-fails { integer }  Maximum missed LCP echo messages before disconnect. range[0-32767]
    set defaultgw { enable | disable }  Enable to get the gateway IP from the DHCP or PPPoE server.
    set dns-server-override { enable | disable }  Enable/disable use DNS acquired by DHCP or PPPoE.
    set auth-type { option }  PPP authentication type to use.
        auto      Automatically choose authentication.
        pap       PAP authentication.

```



```
        chap      CHAP authentication.
        mschapv1  MS-CHAPv1 authentication.
        mschapv2  MS-CHAPv2 authentication.
set ptp-client { enable | disable } Enable/disable PTP client.
set ptp-user { string } PTP user name. size[64]
set ptp-password { password_string } PTP password. size[128]
set ptp-server-ip { ipv4_address } PTP server IP address.
set ptp-auth-type { option } PTP authentication type.
        auto      Automatically choose authentication.
        pap       PAP authentication.
        chap      CHAP authentication.
        mschapv1  MS-CHAPv1 authentication.
        mschapv2  MS-CHAPv2 authentication.
set ptp-timeout { integer } Idle timer in minutes (0 for disabled). range[0-65535]
set arpforward { enable | disable } Enable/disable ARP forwarding.
set ndiscforward { enable | disable } Enable/disable NDISC forwarding.
set broadcast-forward { enable | disable } Enable/disable broadcast forwarding.
set bfd { global | enable | disable } Bidirectional Forwarding Detection (BFD) settings.
set bfd-desired-min-tx { integer } BFD desired minimal transmit interval. range[1-100000]
set bfd-detect-mult { integer } BFD detection multiplier. range[1-50]
set bfd-required-min-rx { integer } BFD required minimal receive interval. range[1-100000]
set l2forward { enable | disable } Enable/disable L2 forwarding.
set icmp-redirect { enable | disable } Enable/disable ICMP redirect.
set vlanforward { enable | disable } Enable/disable traffic forwarding between VLANs on this interface.
set stpforward { enable | disable } Enable/disable STP forwarding.
set stpforward-mode { rpl-all-ext-id | rpl-bridge-ext-id | rpl-nothing } Configure STP forwarding mode.
        rpl-all-ext-id  Replace all extension IDs (root, bridge).
        rpl-bridge-ext-id  Replace the bridge extension ID only.
        rpl-nothing      Replace nothing.
set ips-sniffer-mode { enable | disable } Enable/disable the use of this interface as a one-armed sniffer.
set ident-accept { enable | disable } Enable/disable authentication for this interface.
set ipmac { enable | disable } Enable/disable IP/MAC binding.
set subst { enable | disable } Enable to always send packets from this interface to a destination MAC address.
set macaddr { mac address } Change the interface's MAC address.
set substitute-dst-mac { mac address } Destination MAC address that all packets are sent to from this interface.
set speed { option } Interface speed. The default setting and the options available depend on the interface hardware.
        auto      Automatically adjust speed.
        10full    10M full-duplex.
        10half    10M half-duplex.
        100full   100M full-duplex.
        100half   100M half-duplex.
        1000full  1000M full-duplex.
        1000half  1000M half-duplex.
```

```

    1000auto 1000M auto adjust.
    10000full 10G full-duplex.
set status { up | down } Bring the interface up or shut the interface down.
    up Bring the interface up.
    down Shut the interface down.
set netbios-forward { disable | enable } Enable/disable NETBIOS forwarding.
set wins-ip { ipv4 address } WINS server IP.
set type { option } Interface type.
    physical Physical interface.
    vlan VLAN interface.
    aggregate Aggregate interface.
    redundant Redundant interface.
    tunnel Tunnel interface.
    vdom-link VDOM link interface.
    loopback Loopback interface.
    switch Software switch interface.
    hard-switch Hardware switch interface.
    vap-switch VAP interface.
    wl-mesh WLAN mesh interface.
    fext-wan FortiExtender interface.
    vxlan VXLAN interface.
    hdlc T1/E1 interface.
    switch-vlan Switch VLAN interface.
set dedicated-to { none | management } Configure interface for single purpose.
    none Interface not dedicated for any purpose.
    management Dedicate this interface for management purposes only.
set trust-ip-1 { ipv4 classnet any } Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).
set trust-ip-2 { ipv4 classnet any } Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).
set trust-ip-3 { ipv4 classnet any } Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).
set trust-ip6-1 { ipv6 prefix } Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).
set trust-ip6-2 { ipv6 prefix } Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).
set trust-ip6-3 { ipv6 prefix } Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).
set mtu-override { enable | disable } Enable to set a custom MTU for this interface.
set mtu { integer } MTU value for this interface. range[0-4294967295]
set wccp { enable | disable } Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.
set netflow-sampler { disable | tx | rx | both } Enable/disable NetFlow on this interface and set the data that NetFlow collects (rx, tx, or both).
    disable Disable NetFlow protocol on this interface.
    tx Monitor transmitted traffic on this interface.
    rx Monitor received traffic on this interface.
    both Monitor transmitted/received traffic on this interface.
set sflow-sampler { enable | disable } Enable/disable sFlow on this interface.

```

```
set drop-overlapped-fragment { enable | disable } Enable/disable drop overlapped fragment packets.
set drop-fragment { enable | disable } Enable/disable drop fragment packets.
set scan-botnet-connections { disable | block | monitor } Enable monitoring or blocking connections to Botnet servers through this interface.
    disable Do not scan connections to botnet servers.
    block Block connections to botnet servers.
    monitor Log connections to botnet servers.
set src-check { enable | disable } Enable/disable source IP check.
set sample-rate { integer } sFlow sample rate (10 - 99999). range[10-99999]
set polling-interval { integer } sFlow polling interval (1 - 255 sec). range[1-255]
set sample-direction { tx | rx | both } Data that NetFlow collects (rx, tx, or both).
    tx Monitor transmitted traffic on this interface.
    rx Monitor received traffic on this interface.
    both Monitor transmitted/received traffic on this interface.
set explicit-web-proxy { enable | disable } Enable/disable the explicit web proxy on this interface.
set explicit-ftp-proxy { enable | disable } Enable/disable the explicit FTP proxy on this interface.
set proxy-captive-portal { enable | disable } Enable/disable proxy captive portal on this interface.
set tcp-mss { integer } TCP maximum segment size. 0 means do not change segment size. range[0-4294967295]
set mediatype { serdes-sfp | sgmi-sfp | serdes-copper-sfp } Select SFP media interface type
    serdes-sfp SFP using SerDes Media Interface
    sgmi-sfp SFP using SGMII Media Interface
    serdes-copper-sfp Copper SFP using SerDes media Interface.
set inbandwidth { integer } Bandwidth limit for incoming traffic (0 - 16776000 kbps), 0 means unlimited. range[0-16776000]
set outbandwidth { integer } Bandwidth limit for outgoing traffic (0 - 16776000 kbps). range[0-16776000]
set spillover-threshold { integer } Egress Spillover threshold (0 - 16776000 kbps), 0 means unlimited. range[0-16776000]
set ingress-spillover-threshold { integer } Ingress Spillover threshold (0 - 16776000 kbps). range[0-16776000]
set weight { integer } Default weight for static routes (if route has no weight configured). range[0-255]
set interface { string } Interface name. size[15] - datasource(s): system.interface.name
set external { enable | disable } Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).
set vlanid { integer } VLAN ID (1 - 4094). range[1-4094]
set forward-domain { integer } Transparent mode forward domain. range[0-2147483647]
set remote-ip { ipv4 address any } Remote IP address of tunnel.
config member
    edit { interface-name }
        # Physical interfaces that belong to the aggregate or redundant interface.
        set interface-name { string } Physical interface name. size[64] - datasource(s): system.interface.name
    next
set lACP-mode { static | passive | active } LACP mode.
    static Use static aggregation, do not send and ignore any LACP messages.
    passive Passively use LACP to negotiate 802.3ad aggregation.
    active Actively use LACP to negotiate 802.3ad aggregation.
set lACP-ha-slave { enable | disable } LACP HA slave.
```

```
set lacp-speed { slow | fast } How often the interface sends LACP messages.
    slow Send LACP message every 30 seconds.
    fast Send LACP message every second.
set min-links { integer } Minimum number of aggregated ports that must be up. range[1-32]
set min-links-down { operational | administrative } Action to take when less than the configured minimum number of links are active.
    operational Set the aggregate operationally down.
    administrative Set the aggregate administratively down.
set algorithm { L2 | L3 | L4 } Frame distribution algorithm.
    L2 Use layer 2 address for distribution.
    L3 Use layer 3 address for distribution.
    L4 Use layer 4 information for distribution.
set link-up-delay { integer } Number of milliseconds to wait before considering a link is up. range[50-3600000]
set priority-override { enable | disable } Enable/disable fail back to higher priority port once recovered.
set aggregate { string } Aggregate interface. size[15]
set redundant-interface { string } Redundant interface. size[15]
config managed-device
    edit { name }
        # Available when FortiLink is enabled, used for managed devices through FortiLink interface.
        set name { string } Managed dev identifier. size[64]
    next
set devindex { integer } Device Index. range[0-4294967295]
set vindex { integer } Switch control interface VLAN ID. range[0-65535]
set switch { string } Contained in switch. size[15]
set description { string } Description. size[255]
set alias { string } Alias will be displayed with the interface name to make it easier to distinguish. size[25]
set security-mode { none | captive-portal | 802.1X } Turn on captive portal authentication for this interface.
    none No security option.
    captive-portal Captive portal authentication.
    802.1X 802.1X port-based authentication.
set captive-portal { integer } Enable/disable captive portal. range[0-4294967295]
set security-mac-auth-bypass { enable | disable } Enable/disable MAC authentication bypass.
set security-external-web { string } URL of external authentication web server. size[127]
set security-external-logout { string } URL of external authentication logout server. size[127]
set replacemsg-override-group { string } Replacement message override group. size[35]
set security-redirect-url { string } URL redirection after disclaimer/authentication. size[127]
set security-exempt-list { string } Name of security-exempt-list. size[35]
config security-groups
    edit { name }
        # User groups that can authenticate with the captive portal.
        set name { string } Names of user groups that can authenticate with the captive portal. size[64]
    next
set device-identification { enable | disable } Enable/disable passively gathering of device identity information about the devices on the
network connected to this interface.
```

```
set device-user-identification { enable | disable } Enable/disable passive gathering of user identity information about users on this interface.
set device-identification-active-scan { enable | disable } Enable/disable active gathering of device identity information about the devices on the network connected to this interface.
set device-access-list { string } Device access list. size[35]
set device-netscan { disable | enable } Enable/disable inclusion of devices detected on this interface in network vulnerability scans.
set lldp-transmission { enable | disable | vdom } Enable/disable Link Layer Discovery Protocol (LLDP) transmission.
set fortiheartbeat { enable | disable } Enable/disable FortiHeartBeat (FortiTelemetry on GUI).
set broadcast-forticlient-discovery { enable | disable } Enable/disable broadcasting FortiClient discovery messages.
set endpoint-compliance { enable | disable } Enable/disable endpoint compliance enforcement.
set estimated-upstream-bandwidth { integer } Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization. range[0-4294967295]
set estimated-downstream-bandwidth { integer } Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization. range[0-4294967295]
set vrrp-virtual-mac { enable | disable } Enable/disable use of virtual MAC for VRRP.
config vrrp
  edit { vrid }
    # VRRP configuration.
    set vrid { integer } Virtual router identifier (1 - 255). range[1-255]
    set vrgrp { integer } VRRP group ID (1 - 65535). range[1-65535]
    set vrip { ipv4 address any } IP address of the virtual router.
    set priority { integer } Priority of the virtual router (1 - 255). range[1-255]
    set adv-interval { integer } Advertisement interval (1 - 255 seconds). range[1-255]
    set start-time { integer } Startup time (1 - 255 seconds). range[1-255]
    set preempt { enable | disable } Enable/disable preempt mode.
    set vrdst { ipv4 address any } Monitor the route to this destination.
    set vrdst-priority { integer } Priority of the virtual router when the virtual router destination becomes unreachable (0 - 254). range[0-254]
    set status { enable | disable } Enable/disable this VRRP configuration.
  next
set role { lan | wan | dmz | undefined } Interface role.
  lan Connected to local network of endpoints.
  wan Connected to Internet.
  dmz Connected to server zone.
  undefined Interface has no specific role.
set snmp-index { integer } Permanent SNMP Index of the interface. range[0-4294967295]
set secondary-IP { enable | disable } Enable/disable adding a secondary IP to this interface.
config secondaryip
  edit { id }
    # Second IP address of interface.
    set id { integer } ID. range[0-4294967295]
    set ip { ipv4 classnet host } Secondary IP address of the interface.
    set allowaccess { option } Management access settings for the secondary IP address.
```

```

ping          PING access.
https        HTTPS access.
ssh          SSH access.
snmp         SNMP access.
http         HTTP access.
telnet       TELNET access.
fgfm         FortiManager access.
radius-acct  RADIUS accounting access.
probe-response Probe access.
capwap       CAPWAP access.
ftm          FTM access.
set gwdetect { enable | disable } Enable/disable detect gateway alive for first.
set ping-serv-status { integer } PING server status. range[0-255]
set detectserver { string } Gateway's ping server for this IP.
set detectprotocol { ping | tcp-echo | udp-echo } Protocols used to detect the server.
    ping      PING.
    tcp-echo  TCP echo.
    udp-echo  UDP echo.
set ha-priority { integer } HA election priority for the PING server. range[1-50]
next
set preserve-session-route { enable | disable } Enable/disable preservation of session route when dirty.
set auto-auth-extension-device { enable | disable } Enable/disable automatic authorization of dedicated Fortinet extension device on this
interface.
set ap-discover { enable | disable } Enable/disable automatic registration of unknown FortiAP devices.
set fortilink-stacking { enable | disable } Enable/disable FortiLink switch-stacking on this interface.
set fortilink-split-interface { enable | disable } Enable/disable FortiLink split interface to connect member link to different FortiSwitch
in stack for uplink redundancy (maximum 2 interfaces in the "members" command).
set internal { integer } Implicitly created. range[0-255]
set fortilink-backup-link { integer } fortilink split interface backup link. range[0-255]
set switch-controller-access-vlan { enable | disable } Switch controller access VLAN.
set switch-controller-igmp-snooping { enable | disable } Switch controller IGMP snooping.
set switch-controller-dhcp-snooping { enable | disable } Switch controller DHCP snooping.
set switch-controller-dhcp-snooping-verify-mac { enable | disable } Switch controller DHCP snooping verify MAC.
set switch-controller-dhcp-snooping-option82 { enable | disable } Switch controller DHCP snooping option82.
set switch-controller-auth { usergroup | radius } Switch controller authentication.
    usergroup  User group.
    radius     RADIUS.
set switch-controller-radius-server { string } RADIUS server name for this FortiSwitch VLAN. size[35]
set color { integer } Color of icon on the GUI. range[0-32]
set ip6-mode { static | dhcp | pppoe | delegated } Addressing mode (static, DHCP, delegated).
    static    Static setting.
    dhcp      DHCPv6 client mode.
    pppoe     IPv6 over PPPoE mode.

```

```

        delegated IPv6 address with delegated prefix.
set nd-mode { basic | SEND-compatible } Neighbor discovery mode.
    basic          Do not support SEND.
    SEND-compatible Support SEND.
set nd-cert { string } Neighbor discovery certificate. size[35] - datasource(s): certificate.local.name
set nd-security-level { integer } Neighbor discovery security level (0 - 7; 0 = least secure, default = 0). range[0-7]
set nd-timestamp-delta { integer } Neighbor discovery timestamp delta value (1 - 3600 sec; default = 300). range[1-3600]
set nd-timestamp-fuzz { integer } Neighbor discovery timestamp fuzz factor (1 - 60 sec; default = 1). range[1-60]
set nd-cga-modifier { string } Neighbor discovery CGA modifier.
set ip6-dns-server-override { enable | disable } Enable/disable using the DNS server acquired by DHCP.
set ip6-address { ipv6 prefix } Primary IPv6 address prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx
config ip6-extra-addr
    edit { prefix }
        # Extra IPv6 address prefixes of interface.
        set prefix { ipv6 prefix } IPv6 address prefix.
    next
set ip6-allowaccess { option } Allow management access to the interface.
    ping    PING access.
    https   HTTPS access.
    ssh     SSH access.
    snmp    SNMP access.
    http    HTTP access.
    telnet  TELNET access.
    fgfm    FortiManager access.
    capwap  CAPWAP access.
set ip6-send-adv { enable | disable } Enable/disable sending advertisements about the interface.
set ip6-manage-flag { enable | disable } Enable/disable the managed flag.
set ip6-other-flag { enable | disable } Enable/disable the other IPv6 flag.
set ip6-max-interval { integer } IPv6 maximum interval (4 to 1800 sec). range[4-1800]
set ip6-min-interval { integer } IPv6 minimum interval (3 to 1350 sec). range[3-1350]
set ip6-link-mtu { integer } IPv6 link MTU. range[0-4294967295]
set ip6-reachable-time { integer } IPv6 reachable time (milliseconds; 0 means unspecified). range[0-3600000]
set ip6-retrans-time { integer } IPv6 retransmit time (milliseconds; 0 means unspecified). range[0-4294967295]
set ip6-default-life { integer } Default life (sec). range[0-9000]
set ip6-hop-limit { integer } Hop limit (0 means unspecified). range[0-255]
set autoconf { enable | disable } Enable/disable address auto config.
set ip6-upstream-interface { string } Interface name providing delegated information. size[15] - datasource(s): system.interface.name
set ip6-subnet { ipv6 prefix } Subnet to routing prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx
config ip6-prefix-list
    edit { prefix }
        # Advertised prefix list.
        set prefix { ipv6 network } IPv6 prefix.
        set autonomous-flag { enable | disable } Enable/disable the autonomous flag.

```

```

    set onlink-flag { enable | disable } Enable/disable the onlink flag.
    set valid-life-time { integer } Valid life time (sec). range[0-4294967295]
    set preferred-life-time { integer } Preferred life time (sec). range[0-4294967295]
    set rdns { string } Recursive DNS server option.
    config dnssl
        edit { domain }
            # DNS search list option.
            set domain { string } Domain name. size[79]
        next
    next
config ip6-delegated-prefix-list
    edit { prefix-id }
        # Advertised IPv6 delegated prefix list.
        set prefix-id { integer } Prefix ID. range[0-4294967295]
        set upstream-interface { string } Name of the interface that provides delegated information. size[15] - datasource(s): sys-
tem.interface.name
        set autonomous-flag { enable | disable } Enable/disable the autonomous flag.
        set onlink-flag { enable | disable } Enable/disable the onlink flag.
        set subnet { ipv6 network } Add subnet ID to routing prefix.
        set rdns-service { delegated | default | specify } Recursive DNS service option.
            delegated Delegated RDNSS settings.
            default System RDNSS settings.
            specify Specify recursive DNS servers.
        set rdns { string } Recursive DNS server option.
    next
set dhcp6-relay-service { disable | enable } Enable/disable DHCPv6 relay.
set dhcp6-relay-type { regular } DHCPv6 relay type.
    regular Regular DHCP relay.
set dhcp6-relay-ip { string } DHCPv6 relay IP address.
set dhcp6-client-options { rapid | iapd | iana } DHCPv6 client options.
    rapid Send rapid commit option.
    iapd Send including IA-PD option.
    iana Send including IA-NA option.
set dhcp6-prefix-delegation { enable | disable } Enable/disable DHCPv6 prefix delegation.
set dhcp6-information-request { enable | disable } Enable/disable DHCPv6 information request.
set dhcp6-prefix-hint { ipv6 network } DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.
set dhcp6-prefix-hint-plt { integer } DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time. range[0-4294967295]
set dhcp6-prefix-hint-vlt { integer } DHCPv6 prefix hint valid life time (sec). range[0-4294967295]
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

vdom <string>

Vdom name to which this interface belong, default is root.

mode {static | dhcp | pppoe}

The interface IP addressing: static, from external dhcp or external pppoe.

distance <integer>

The administrative distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route for the same destination, value between 1 to 255.

priority <integer>

The priority of routes using this interface, lower priority indicates preferred route for the same destination, value between 0 to 4294967295, available when mode set to DHCP or PPPoE.

dhcp-relay-ip <ip>

The IP of DHCP relay server.

dhcp-relay-service {disable | enable}

Disable or enable DHCP relay service on this interface, default is disable.

dhcp-relay-type {regular | ipsec}

Set a regular or an IPsec relay type on this interface.

dhcp-client-identifier <string>

Used to override the default DHCP client ID created by the FortiGate.

ip <ip & netmask>

The interface's IP and subnet mask, syntax: X.X.X.X/24.

allowaccess {ping | https | ssh | snmp | http | telnet | ...}

Permitted access type on this interface:

- fgfm: FortiManager access.
 - radius-acct: RADIUS accounting access.
 - probe-response: Probe access.
 - capwap: CAPWAP access.
-

fail-detect {enable | disable}

Enable or disable interface failed options.

fail-detect-option {detectserver | link-down}

Select whether the FortiGate detects interface failure by ping server (detectserver) or port detection (link-down), detectserver is only available in NAT mode.

fail-alert-method {link-failed-signal | link-down}

Select link-failed-signal or link-down method to alert about a failed link.

fail-alert-interfaces {port1 | port2 | ...}

The names of the FortiGate interfaces from which the link failure alert is sent for this interface.

ipunnumbered <ip>

The Unnumbered IP used for PPPoE interfaces for which no unique local address is provided. If you have been assigned a block of IP addresses by your ISP you can add any of these IP.

username <string>

The username of the PPPoE account, provided by your ISP.

password <passwd>

The PPPoE account's password.

idle-timeout <integer>

Idle time in seconds after which the PPPoE session is disconnected, 0 for no timeout.

disc-retry-timeout <integer>

The time in seconds to wait before retrying to start a PPPoE discovery, 0 to disable this feature.

padt-retry-timeout <integer>

PPPoE Active Discovery Terminate (PADT) timeout in seconds used to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP.

service-name <string>

Set a name for this PPPoE service.

ac-name <string>

Set the PPPoE server name.

lcp-echo-interval <integer>

The time in seconds between PPPoE Link Control Protocol (LCP) echo requests, default is 5.

lcp-max-echo-fails <integer>

Maximum number of missed LCP echoes before the PPPoE link is disconnected, default is 3.

defaultgw {enable | disable}

Enable to get the gateway IP from the DHCP or PPPoE server, default is enable.

dns-server-override {enable | disable}

Disable to prevent this interface from using a DNS server acquired via DHCP or PPPoE, default is enable.

pptp-client {enable | disable}

Enable or disable the use of point-to-point tunneling protocol (PPTP) client, available in static mode only, default is disable.

pptp-user <string>

PPTP end user name.

pptp-password <passwd>

PPTP end user password.

pptp-server-ip <ip>

PPTP server's IP address.

pptp-auth-type {auto | pap | chap | mschapv1 | mschapv2}

The server authentication type, default is auto.

pptp-timeout <integer>

Idle timeout in minutes to shut down the PPTP session, values between 0 to 65534 (65534 minutes is 45 days), 0 for disabled, default is 0.

arpforward {enable | disable}

Enable or disable ARP packets forwarding on this interface, default is enable.

broadcast-forward {enable | disable}

Enable or disable automatic forwarding of broadcast packets, default is disable.

priority-override {enable | disable}

Enable or disable fail back to higher priority port once recovered. Once enabled, `priority-override` on redundant interfaces gives greater priority to interfaces that are higher in the member list.

bfd {global | enable | disable}

Use the global setting, enable, or disable Bidirectional Forwarding Detection (bfd) on this interface, global bfd settings is in config system settings, default is global.

l2forward {enable | disable}

Enable or disable layer-2 forwarding for this interface, default is disable.

icmp-redirect {enable | disable}

Enable or disable sending ICMP redirect messages from this interface, FortiGate send ICMP redirect messages to notify the original sender of packets if there is a better route available, default is enable.

vlanforward {enable | disable}

Enable or disable traffic forwarding between VLANs on this interface, default is disable.

stpforward {enable | disable}

Enable or disable Spanning Tree Protocol (STP) packets forward. STP creates a spanning tree within a network of connected layer-2 bridges while disabling all other links, leaving a single active path between any two network nodes to prevent any loops which would flood the network.

stpforward-mode {rpl-all-ext-id | rpl-bridge-ext-id | ...}

Set the STP forward mode:

- rpl-all-ext-id: Replace all root and bridge extension IDs, the default mode.
 - rpl-bridge-ext-id : Replace the bridge extension ID only.
 - rpl-nothing: Do not replace anything.
-

ips-sniffer-mode {enable | disable}

Enable or disable the use of this interface as a one-armed sniffer as part of configuring a FortiGate unit to operate as an IDS appliance by sniffing packets for attacks without processing packets. when enabled you cannot use the interface for other traffic, default is disable.

ident-accept {enable | disable}

Enable or disable passing packets identification on TCP port 113 to the firewall policy used to determine a user's identity on a particular TCP connection, default is disable. Enable or disable passing packets identification on TCP port 113 to the firewall policy used to determine a user's identity on a particular TCP connection, default is disable.

switch-controller-access-vlan {enable | disable}

Note: This setting's definition has been modified from a previous release.

VLAN access status:

- enable: Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.
 - disable: Allow normal VLAN traffic.
-

ipmac {enable | disable}

Enable or disable IP/MAC binding for the specified interface, default is disable. More information available in `config firewall ipmacbinding setting` command.

subst {enable | disable}

Enable to always send packets from this interface to the same destination MAC address. Use `substitute-dst-mac` to set the destination MAV address. Disabled by default.

macaddr <mac>

Override the factory MAC address of this interface by specifying a new MAC address.

substitute-dst-mac <mac>

The destination MAC address that all packets are sent to from this interface if `subst` is enabled.

speed {auto | 10full | 10half | etc }

The interface speed. The default setting and the speeds available depend on the interface hardware. Most often speed is set to `auto` and the interface negotiates with connected equipment to select the best speed. You can set specific speeds if the connected equipment doesn't support negotiation. Some FortiGate interface hardware does not support `auto`. In which case set the interface speed to match the connected network equipment speed.

Enter a space and a "?" after the speed field to display a list of speeds available for your model and interface.

status {up | down}

Start or stop the interface, when stopped, it does not accept or send packets.

If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.

netbios-forward {disable | enable}

Enable to forward Network Basic Input Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server. Enable to forward Network Basic Input Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server.

wins-ip <ip>

The IP address of a WINS server to which NetBIOS broadcasts is forwarded.

type <interface-type>

Enter set type ? to see a list of the interface types that can be created.

mtu-override {enable | disable}

Select `enable` to use custom MTU size instead of default 1 500.

mtu <integer>

Set a new MTU value.

wccp {enable | disable}

Enable or disable Web Cache Communication Protocol (WCCP) on this interface, default is disable.

netflow-sampler {disable | tx | rx | both}

Disable or choose how to use netflow on this interface:

- tx: Monitor transmitted traffic.
 - rx: Monitor received traffic.
 - both: Monitor both direction traffic.
-

sflow-sampler {enable | disable}

Enable or disable sflow protocol on this interface, default is disable. More information on sflow in `config system sflow` command.

drop-overlapped-fragment {enable | disable}

Enable or disable dropping overlapped packet fragments, default is disable.

drop-fragment {enable | disable}

Enable to drop fragmented packets, default is disable.

scan-botnet-connections {disable | block | monitor}

Disable or choose how to handle connections to botnet servers:

- block: Terminate connections
 - monitor: Log connections.
-

sample-rate <integer>

The sample rate defines the average number of packets to wait between samples, value between 10 to 99999. For example, the default sample-rate of 2000 samples 1 of every 2000 packets.

The lower the sample-rate the higher the number of packets sampled. Sampling more packets increases the accuracy of the sampling data but also increases the CPU and network bandwidth required to support sFlow. The default sample-rate of 2000 provides high enough accuracy in most cases.

polling-interval <integer>

The amount of time in seconds that the sFlow agent waits between sending collected data to the sFlow collector, value between 1 to 255.

A higher polling-interval means less data is sent across the network but also means that the sFlow collector's picture of the network may be out of date, default is 20.

sample-direction {tx | rx | both}

Configure the sFlow agent to sample traffic received by the interface (rx) or sent from the interface (tx) or both.

explicit-web-proxy {enable | disable}

Enable or disable explicit Web proxy on this interface, default is disable.

explicit-ftp-proxy {enable | disable}

Enable or disable explicit FTP proxy on this interface, default is disable.

tcp-mss <integer>

The Maximum Size Segment (mss) for TCP connections, it is used when there is an MTU mismatch or DF (Don't Fragment) bit is set.

inbandwidth <integer>

The limit of ingress traffic, in Kbit/sec, on this interface, default is 0 which indicate unlimited.

outbandwidth <integer>

The limit of egress traffic, in Kbit/sec, on this interface, default is 0 which indicate unlimited.

spillover-threshold <integer>

Egress Spillover threshold in kbps used for load balancing traffic between interfaces, range from 0 to 16776000, default is 0.

ingress-spillover-threshold <integer>

Ingress Spillover threshold in kbps, range from 0 to 16776000, default is 0.

weight <integer>

Set the default weight for static routes on this interface. This applies when the route has no weight configured.

external {enable | disable}

Enable or disable identifying if this interface is connected to external side.

config managed-device

Available when `fortilink` is enabled, used for managed devices through fortalink interface.

edit <name>

The identifier of the managed device.

description <string>

Optionally describe this interface.

alias <string>

Optionally set an alias which will be displayed with the interface name to make it easier to distinguish.

l2tp-client {enable | disable}

Enable or disable this interface as a Layer 2 Tunneling Protocol (L2TP) client.

You may need to enable l2forward on this interface, default is disable.

security-mode {none | captive-portal}

Available when `fortilink` is disabled, `captive-portal` allow access to only authenticated members through this interface.

security-mac-auth-bypass {enable | disable}

Enable or disable MAC address authentication bypass.

security-external-web <string>

The URL of an external authentication web server, available when `security-mode` is set to `captive-portal`.

security-external-logout <string>

The URL of an external authentication logout server, available when `security-mode` is set to `captive-portal`.

replacemsg-override-group <group-name>

Specify replacement message override group name, this is for captive portal messages when `security-mode` is set to `captive-portal`.

security-redirect-url <string>

Specify URL redirection after captive portal authentication or disclaimer.

security-groups <user-group>

Optionally, enter the groups that are allowed access to this interface.

security-exempt-list <name>

Optionally specify the members will bypass the captive portal authentication.

device-identification {enable | disable}

Enable or disable passive gathering of identity information about source hosts on this interface.

device-user-identification {enable | disable}

Enable or disable passive gathering of user identity information about source hosts on this interface.

device-identification-active-scan {enable | disable}

Enable or disable active gathering of identity information about source hosts on this interface.

device-access-list <name>

Specify the device access list to use which is configured in `config user device-access-list`.

lldp-transmission {enable | disable | vdom}

Enable, disable, or apply to vdom-level the Link Layer Discovery Protocol (LLDP) transmission for this interface, default is vdom.

fortiheartbeat {enable | disable}

Enable or disable FortiHeartBeat (FortiTelemetry on GUI) which used to listen for connections from devices with FortiClient installed, default is disable.

broadcast-forticlient-discovery {enable | disable}

Enable or disable broadcast FortiClient discovery messages, default is disable.

endpoint-compliance {enable | disable}

Enable or disable endpoint compliance enforcement, default is disabled.

estimated-upstream-bandwidth <integer>

Estimated maximum upstream bandwidth in kbps, used to estimate link utilization.

estimated-downstream-bandwidth <integer>

Estimated maximum downstream bandwidth in kbps, used to estimate link utilization.

vrrp-virtual-mac {enable | disable}

Enable or disable the Virtual Router Redundancy Protocol (VRRP) virtual MAC addresses for the VRRP routers added to this interface, default is disable. See [RFC3768](#) For more information about VRRP.

config vrrp**vrgroup <integer>**

VRRP group id.

vrip <ip>

IP of the virtual router.

priority <integer>

Virtual router's priority, value between 1 to 255, default is 100.

adv-interval <integer>

Advertisement interval in seconds, value between 1 to 255

start-time <integer>

Startup time in seconds, value between 1 to 255, default is 3.

preempt {enable | disable}

Enable or disable preempt mode, default is enable.

vrdst <ip>

Monitor the route to this destination.

status {enable | disable}

Enabled by default.

role {lan | wan | dmz | undefined}

Optionally choose the interface role: lan: Connected to local network of endpoints. wan: Connected to Internet. dmz: Connected to server zone. undefined: Interface has no specific role.

snmp-index <integer>

Optionally set a permanent SNMP Index of this interface.

secondary-IP {enable | disable}

Enable or disable the use of a secondary address on this interface.

config secondaryip

ip <ip & netmask>

The interface's secondary IP and subnet mask, syntax: X.X.X.X/24.

allowaccess {ping | https | ssh | snmp | http | telnet | ...}

Permitted access type on this secondary IP:

- fgfm: FortiManager access.
- radius-acct: RADIUS accounting access.
- probe-response: Probe access.
- capwap: CAPWAP access.

auto-auth-extension-device {enable | disable}

Enable or disable automatic authorization of dedicated Fortinet extension devices on this interface, default is disabled.

ap-discover {enable | disable}

Enable or disable automatic registration of unknown FortiAP devices, default is disable.

fortilink {enable | disable}

Enable or disable FortiLink on this interface to manage other Fortinet devices such as FortiSwitch.

fortilink-stacking {enable | disable}

Enable or disable FortiLink switch-stacking on this interface.

config ipv6

ip6-mode {static | dhcp | delegated}

The addressing mode:

- static: Static setting, default mode.
- dhcp: DHCPv6 client.
- delegated: IPv6 address with delegated prefix.

ip6-dns-server-override {enable | disable}

Enable or disable using DNS acquired by DHCP.

ip6-address <ipv6>

Primary IPv6 address prefix of this interface.

config ip6-extra-addr

edit <prefix>

IPv6 address prefix.

ip6-allowaccess {ping | https | ssh | snmp | http | ...}

Allow management access to the interface:

- fgfm: FortiManager access.
- capwap: CAPWAP access.

ip6-send-adv {enable | disable}

Enable or disable the flag indicating whether or not to send periodic router advertisements and to respond to router solicitations. When enabled, this interface's address will be added to all-routers group (FF02::02) and be included in an Multi Listener Discovery (MLD) report. If no interfaces on the FortiGate unit have ip6-send-adv enabled, the FortiGate unit will only listen to the all-hosts group (FF02::01) which is explicitly excluded from MLD reports according to [RFC 2710](#) section 5.

When disabled (by default), and autoconf is enabled, the FortiGate unit acts as a stateless address auto-configuration client (SLAAC).

ip6-manage-flag {enable | disable}

Enable or disable the managed address configuration flag in router advertisements, default is enable.

ip6-other-flag {enable | disable}

Enable or disable the other stateful configuration flag in router advertisements, default is enable.

ip6-max-interval <integer>

The maximum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface, value between 4 to 1800, default is 600.

ip6-min-interval <integer>

The minimum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface, value between 3 to 1350, default is 198.

ip6-link-mtu <integer>

The link MTU to be added to the router advertisements options field, 0 means that no MTU options are sent.

ip6-reachable-time <integer>

The time, in milliseconds, to be added to the reachable time field in the router advertisements, value between 0 to 3600000, default is 0 which mean no reachable time is specified.

ip6-retrans-time <integer>

The number, in milliseconds, to be added to the Retrans Timer field in the router advertisements, default is 0 which mean that the Retrans Timer is not specified.

ip6-default-life <integer>

The time, in seconds, to be added to the Router Lifetime field of router advertisements sent from the interface, default is 1800.

config ip6-prefix-list

edit <prefix>

Enter the IPv6 prefix you want to configure.

autonomous-flag {enable | disable}

Set the state of the autonomous flag for this IPv6 prefix, default is disable.

onlink-flag {enable | disable}

Set the state of the on-link flag in this IPv6 prefix, default is disable.

valid-life-time <integer>

The valid lifetime in seconds for this IPv6 prefix, default is 2592000 (30 days).

preferred-life-time <integer>

The preferred lifetime in seconds, default is 604800 (7 days).

config ip6-delegated-prefix-list

edit <prefix-id>

An ID (integer) for this ip6 delegated prefix.

upstream-interface <interface>

The interface name from where delegated information is provided.

autonomous-flag {enable | disable}

Set the state of the autonomous flag for this IPv6 delegated prefix, default is disable.

onlink-flag {enable | disable}

Set the state of the on-link flag in this IPv6 delegated prefix, default is disable.

subnet <ipv6_net>

Subnet to routing prefix, syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx

ip6-hop-limit <integer>

The number to be added to the Cur Hop Limit field in the router advertisements sent out this interface, default is 0 which mean no hop limit is specified.

nd-mode {basic | SEND-compatible}

Neighbor discovery mode, default is basic.

dhcp6-relay-service {disable | enable}

Enable or disable DHCP relay service for IPv6.

dhcp6-relay-type {regular}

Regular DHCP relay.

dhcp6-relay-ip <ipv6>

The IPv6 of one or more DHCP relays.

dhcp6-prefix-delegation {disable | enable}

Enable or disable DHCPv6 prefix delegation, default is disable.

dhcp6-prefix-hint <ipv6_net>

DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.

dhcp6-prefix-hint-plt <integer>

DHCPv6 prefix hint preferred life time in seconds, default is 604800 (7 days).

dhcp6-prefix-hint-vlt <integer>

DHCPv6 prefix hint valid life time in seconds, default is 2592000 (30 days).

config l2tp-client-settings**user <string>**

L2TP user name.

Password <passwd>

L2TP password.

peer-host <string>

The host name.

peer-mask <netmask>

The netmask.

peer-port <integer>

The port used to connect to L2TP peers, default is 1701.

auth-type {auto | pap | chap | mschapv1 | mschapv2}

Type of authentication used with this client:

- auto— automatically choose type of authentication (default).
- pap — use Password Authentication Protocol.
- chap — use Challenge-Handshake Authentication Protocol.
- mschapv1 — use Microsoft version of CHAP version 1.
- mschapv2 — use Microsoft version of CHAP version 2.

mtu <integer>

The Maximum Transmission Unit (MTU), value between 40 and 65535, default is 1460.

distance <integer>

The administration distance of learned routes, value between 1 to 255, default is 2.

priority <integer>

The routes priority learned through L2TP.

defaultgw {enable | disable}

Enable or disable the use the default gateway, default is disable.

system ipip-tunnel

Introduction.

```
config system ipip-tunnel
  edit { name }
  # Configure IP in IP Tunneling.
  set name { string } IPIP Tunnel name. size[15]
  set interface { string } Interface name that is associated with the incoming traffic from available options. size[15] - datasource(s): system.interface.name
  set remote-gw { ipv4 address } IPv4 address for the remote gateway.
  set local-gw { ipv4 address any } IPv4 address for the local gateway.
  set auto-asic-offload { enable | disable } Enable/disable tunnel ASIC offloading.
next
end
```

system ips-urlfilter-dns

Introduction.

```
config system ips-urlfilter-dns
  edit { address }
  # Configure IPS URL filter DNS servers.
  set address { ipv4 address }  DNS server IP address.
  set status { enable | disable }  Enable/disable using this DNS server for IPS URL filter DNS queries.
next
end
```


system ipv6-neighbor-cache

Introduction.

```
config system ipv6-neighbor-cache
  edit { id }
  # Configure IPv6 neighbor cache table.
  set id { integer } Unique integer ID of the entry. range[0-4294967295]
  set interface { string } Select the associated interface name from available options. size[15] - datasource(s): system.interface.name
  set ipv6 { ipv6 address } IPv6 address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).
  set mac { mac address } MAC address (format: xx:xx:xx:xx:xx:xx).
  next
end
```

system ipv6-tunnel

Introduction.

```
config system ipv6-tunnel
  edit { name }
  # Configure IPv6/IPv4 in IPv6 tunnel.
  set name { string } IPv6 tunnel name. size[15]
  set source { ipv6 address } Local IPv6 address of the tunnel.
  set destination { ipv6 address } Remote IPv6 address of the tunnel.
  set interface { string } Interface name. size[15] - datasource(s): system.interface.name
  set auto-asic-offload { enable | disable } Enable/disable tunnel ASIC offloading.
  next
end
```

system link-monitor

Use this command to add link health monitors that are used to determine the health of an interface. Link health monitors can also be used for FGCP HA remote link monitoring.

```

config system link-monitor
  edit { name }
  # Configure Link Health Monitor.
  set name { string } Link monitor name. size[35]
  set srcintf { string } Interface that receives the traffic to be monitored. size[15] - datasource(s): system.interface.name
  config server
    edit { address }
    # IP address of the server(s) to be monitored.
    set address { string } Server address. size[64]
    next
  set protocol { option } Protocols used to monitor the server.
    ping PING link monitor.
    tcp-echo TCP echo link monitor.
    udp-echo UDP echo link monitor.
    http HTTP-GET link monitor.
    twamp TWAMP link monitor.
  set port { integer } Port number of the traffic to be used to monitor the server. range[1-65535]
  set gateway-ip { ipv4 address any } Gateway IP address used to PING the server.
  set source-ip { ipv4 address any } Source IP address used in packet to the server.
  set http-get { string } 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. size[1024]
  set http-match { string } String that you expect to see in the HTTP-GET requests of the traffic to be monitored. size[1024]
  set interval { integer } Detection interval (1 - 3600 sec, default = 5). range[1-3600]
  set timeout { integer } Detection request timeout (1 - 255 sec, default = 1). range[1-255]
  set failtime { integer } Number of retry attempts before the server is considered down (1 - 10, default = 5) range[1-10]
  set recoverytime { integer } Number of successful responses received before server is considered recovered (1 - 10, default = 5). range[1-
10]
  set security-mode { none | authentication } Twamp controller security mode.
    none Unauthenticated mode.
    authentication Authenticated mode.
  set password { password_string } Twamp controller password in authentication mode size[128]
  set packet-size { integer } Packet size of a twamp test session, range[64-1024]
  set ha-priority { integer } HA election priority (1 - 50). range[1-50]
  set update-cascade-interface { enable | disable } Enable/disable update cascade interface.

```

```
    set update-static-route { enable | disable }  Enable/disable updating the static route.
    set status { enable | disable }  Enable/disable this link monitor.
  next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

srcintf <interface>

The name of the interface to add the link health monitor to.

server <address> [<address>...]

One or more IP addresses of the servers to be monitored. If the link health monitor cannot connect to all of the servers remote IP monitoring considers the link to be down. You can add multiple IP addresses to a single link monitor to monitor more than one IP address from a single interface. If you add multiple IP addresses, the health checking will be with all of the addresses at the same time. The link monitor only fails when no responses are received from all of the addresses.

protocol {ping | tcp-echo | udp-echo | http | twamp}

One or more protocols to be used to test the link. The default is `ping`.

gateway-ip <address>

The IP address of the remote gateway that the link monitor must communicate with to contact the server. Only required if there is no other route on for this communication.

source-ip <address>

Optionally add a source address for the monitoring packets. Normally the source address is the address of the source interface. You can add a different source address if required.

interval <interval>

The time between sending link health check packets. Default is 5 seconds. Range is 1 to 3600 seconds.

timeout <timeout>

The time to wait before receiving a response from the server. Default is 1 second. Range is 1 to 255 seconds.

failtime <failover-threshold>

The number of times that a health check can fail before a failure is detected (the failover threshold). Default is 5. Range is 1 to 10.

recoverytime <recovery-threshold>

The number of times that a health check must succeed after a failure is detected to verify that the server is back up. Default is 5. Range is 1 to 10.

ha-priority <priority>

The priority of this link health monitor when the link health monitor is part of an FGCP remote link monitor configuration. Default is 1. Range is 1 to 50.

update-cascade-interface {disable | enable}

Enable to bring down the source interface if the link health monitor fails. Disable to keep the interface up if the link health monitor fails. Default is enable.

update-static-route {disable | enable}

Enable to remove static routes from the routing table that use this interface if the link monitor fails. Default is enable.

status {disable | enable}

Enable or disable this link health monitor. Default is enable.

system lte-modem

Introduction.

```
config system lte-modem
  set status { enable | disable }  Enable/disable USB LTE/WIMAX device.
  set extra-init { string }  Extra initialization string for USB LTE/WIMAX devices. size[127]
  set authtype { none | pap | chap }  Authentication type for PDP-IP packet data calls.
    none  Username and password not required.
    pap   Use PAP authentication.
    chap  Use CHAP authentication.
  set username { string }  Authentication username for PDP-IP packet data calls. size[63]
  set passwd { password_string }  Authentication password for PDP-IP packet data calls. size[128]
  set apn { string }  Login APN string for PDP-IP packet data calls. size[127]
  set modem-port { integer }  Modem port index (0 - 20). range[0-20]
  set mode { standalone | redundant }  Modem operation mode.
    standalone  Standalone modem operation mode.
    redundant   Redundant modem operation mode where the modem is used as a backup interface.
  set holddown-timer { integer }  Hold down timer (10 - 60 sec). range[10-60]
  set interface { string }  The interface that the modem is acting as a redundant interface for. size[63] - datasource(s): system.interface.name
end
```

system mac-address-table

Introduction.

```
config system mac-address-table
  edit { mac }
  # Configure MAC address tables.
  set mac { mac address }  MAC address.
  set interface { string }  Interface name. size[35] - datasource(s): system.interface.name
  set reply-substitute { mac address }  New MAC for reply traffic.
next
end
```

system management-tunnel

Introduction.

```
config system management-tunnel
  set status { enable | disable }  Enable/disable FGFM tunnel.
  set allow-config-restore { enable | disable }  Enable/disable allow config restore.
  set allow-push-configuration { enable | disable }  Enable/disable push configuration.
  set allow-push-firmware { enable | disable }  Enable/disable push firmware.
  set allow-collect-statistics { enable | disable }  Enable/disable collection of run time statistics.
  set authorized-manager-only { enable | disable }  Enable/disable restriction of authorized manager only.
  set serial-number { string }  Serial number.
end
```


system mobile-tunnel

Introduction.

```

config system mobile-tunnel
  edit { name }
    # Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.
    set name { string } Tunnel name. size[15]
    set status { disable | enable } Enable/disable this mobile tunnel.
    set roaming-interface { string } Select the associated interface name from available options. size[15] - datasource(s): sys-
tem.interface.name
    set home-agent { ipv4 address } IPv4 address of the NEMO HA (Format: xxx.xxx.xxx.xxx).
    set home-address { ipv4 address } Home IP address (Format: xxx.xxx.xxx.xxx).
    set renew-interval { integer } Time before lifetime expiration to send NEMO HA re-registration (5 - 60, default = 60). range[5-60]
    set lifetime { integer } NEMO HA registration request lifetime (180 - 65535 sec, default = 65535). range[180-65535]
    set reg-interval { integer } NEMO HA registration interval (5 - 300, default = 5). range[5-300]
    set reg-retry { integer } Maximum number of NEMO HA registration retries (1 to 30, default = 3). range[1-30]
    set n-mhae-spi { integer } NEMO authentication SPI (default: 256). range[0-4294967295]
    set n-mhae-key-type { ascii | base64 } NEMO authentication key type (ascii or base64).
        ascii The authentication key is an ASCII string.
        base64 The authentication key is Base64 encoded.
    set n-mhae-key { string } NEMO authentication key.
    set hash-algorithm { hmac-md5 } Hash Algorithm (Keyed MD5).
        hmac-md5 Keyed MD5.
    set tunnel-mode { gre } NEMO tunnel mode (GRE tunnel).
        gre GRE tunnel.
  config network
    edit { id }
      # NEMO network configuration.
      set id { integer } Network entry ID. range[0-4294967295]
      set interface { string } Select the associated interface name from available options. size[15] - datasource(s): sys-
tem.interface.name
      set prefix { ipv4 classnet } Class IP and Netmask with correction (Format:xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/x).
      next
    next
  end

```

system modem

Introduction.

```
config system modem
  set status { enable | disable }  Enable/disable Modem support (equivalent to bringing an interface up or down).
  set pin-init { string }  AT command to set the PIN (AT+PIN={ pin }). size[127]
  set network-init { string }  AT command to set the Network name/type (AT+COPS={ mode },[{ format }],[{ oper }],[{ AcT }])). size[127]
  set lockdown-lac { string }  Allow connection only to the specified Location Area Code (LAC). size[127]
  set mode { standalone | redundant }  Set MODEM operation mode to redundant or standalone.
    standalone Standalone.
    redundant Redundant for an interface.
  set auto-dial { enable | disable }  Enable/disable auto-dial after a reboot or disconnection.
  set dial-on-demand { enable | disable }  Enable/disable to dial the modem when packets are routed to the modem interface.
  set idle-timer { integer }  MODEM connection idle time (1 - 9999 min, default = 5). range[1-9999]
  set redial { option }  Redial limit (1 - 10 attempts, none = redial forever).
    none Forever.
    1 One attempt.
    2 Two attempts.
    3 Three attempts.
    4 Four attempts.
    5 Five attempts.
    6 Six attempts.
    7 Seven attempts.
    8 Eight attempts.
    9 Nine attempts.
    10 Ten attempts.
  set reset { integer }  Number of dial attempts before resetting modem (0 = never reset). range[0-10]
  set holddown-timer { integer }  Hold down timer in seconds (1 - 60 sec). range[1-60]
  set connect-timeout { integer }  Connection completion timeout (30 - 255 sec, default = 90). range[30-255]
  set interface { string }  Name of redundant interface. size[63] - datasource(s): system.interface.name
  set wireless-port { integer }  Enter wireless port number, 0 for default, 1 for first port, ... (0 - 4294967295, default = 0) range[0-4294967295]
  set dont-send-CR1 { enable | disable }  Do not send CR when connected (ISP1).
  set phonel { string }  Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters). size[63]
  set dial-cmdl { string }  Dial command (this is often an ATD or ATDT command). size[63]
  set username1 { string }  User name to access the specified dialup account. size[63]
  set passwd1 { password_string }  Password to access the specified dialup account. size[128]
```

```
set extra-init1 { string } Extra initialization string to ISP 1. size[127]
set peer-modem1 { generic | actiontec | ascend_TNT } Specify peer MODEM type for phone1.
    generic All other modem type.
    actiontec ActionTec modem.
    ascend_TNT Ascend TNT modem.
set ppp-echo-request1 { enable | disable } Enable/disable PPP echo-request to ISP 1.
set authtype1 { pap | chap | mschap | mschapv2 } Allowed authentication types for ISP 1.
    pap PAP
    chap CHAP
    mschap MSCHAP
    mschapv2 MSCHAPv2
set dont-send-CR2 { enable | disable } Do not send CR when connected (ISP2).
set phone2 { string } Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).
size[63]
set dial-cmd2 { string } Dial command (this is often an ATD or ATDT command). size[63]
set username2 { string } User name to access the specified dialup account. size[63]
set passwd2 { password_string } Password to access the specified dialup account. size[128]
set extra-init2 { string } Extra initialization string to ISP 2. size[127]
set peer-modem2 { generic | actiontec | ascend_TNT } Specify peer MODEM type for phone2.
    generic All other modem type.
    actiontec ActionTec modem.
    ascend_TNT Ascend TNT modem.
set ppp-echo-request2 { enable | disable } Enable/disable PPP echo-request to ISP 2.
set authtype2 { pap | chap | mschap | mschapv2 } Allowed authentication types for ISP 2.
    pap PAP
    chap CHAP
    mschap MSCHAP
    mschapv2 MSCHAPv2
set dont-send-CR3 { enable | disable } Do not send CR when connected (ISP3).
set phone3 { string } Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).
size[63]
set dial-cmd3 { string } Dial command (this is often an ATD or ATDT command). size[63]
set username3 { string } User name to access the specified dialup account. size[63]
set passwd3 { password_string } Password to access the specified dialup account. size[128]
set extra-init3 { string } Extra initialization string to ISP 3. size[127]
set peer-modem3 { generic | actiontec | ascend_TNT } Specify peer MODEM type for phone3.
    generic All other modem type.
    actiontec ActionTec modem.
    ascend_TNT Ascend TNT modem.
set ppp-echo-request3 { enable | disable } Enable/disable PPP echo-request to ISP 3.
set altmode { enable | disable } Enable/disable altmode for installations using PPP in China.
set authtype3 { pap | chap | mschap | mschapv2 } Allowed authentication types for ISP 3.
    pap PAP
```

```
    chap      CHAP
    mschap    MSCHAP
    mschapv2  MSCHAPv2
set traffic-check { enable | disable }  Enable/disable traffic-check.
set action { dial | stop | none }  Dial up/stop MODEM.
    dial  Dial up number.
    stop  Stop dialup.
    none  No action.
set distance { integer }  Distance of learned routes (1 - 255, default = 1). range[1-255]
set priority { integer }  Priority of learned routes (0 - 4294967295, default = 0). range[0-4294967295]
end
```

system nat64

Introduction.

```
config system nat64
  set status { enable | disable }  Enable/disable NAT64 (default = disable).
  set nat64-prefix { ipv6 prefix }  NAT64 prefix must be ::/96 (default = 64:ff9b::/96).
  set always-synthesize-aaaa-record { enable | disable }  Enable/disable AAAA record synthesis (default = enable).
  set generate-ipv6-fragment-header { enable | disable }  Enable/disable IPv6 fragment header generation.
end
```

system netflow

Introduction.

```
config system netflow
  set collector-ip { ipv4 address } Collector IP.
  set collector-port { integer } NetFlow collector port number. range[0-65535]
  set source-ip { ipv4 address } Source IP address for communication with the NetFlow agent.
  set active-flow-timeout { integer } Timeout to report active flows (1 - 60 min, default = 30). range[1-60]
  set inactive-flow-timeout { integer } Timeout for periodic report of finished flows (10 - 600 sec, default = 15). range[10-600]
  set template-tx-timeout { integer } Timeout for periodic template flowset transmission (1 - 1440 min, default = 30). range[1-1440]
  set template-tx-counter { integer } Counter of flowset records before resending a template flowset record. range[10-6000]
end
```

system network-visibility

Introduction.

```
config system network-visibility
  set destination-visibility { disable | enable }  Enable/disable logging of destination visibility.
  set source-location { disable | enable }  Enable/disable logging of source geographical location visibility.
  set destination-hostname-visibility { disable | enable }  Enable/disable logging of destination hostname visibility.
  set hostname-ttl { integer }  TTL of hostname table entries (60 - 86400). range[60-86400]
  set hostname-limit { integer }  Limit of the number of hostname table entries (0 - 50000). range[0-50000]
  set destination-location { disable | enable }  Enable/disable logging of destination geographical location visibility.
end
```

system np6

Configure a wide range of settings for your FortiGate's NP6 processors including enabling/disabling fastpath and low latency, enabling session accounting and adjusting session timeouts. As well you can set anomaly checking for IPv4 and IPv6 traffic. You can also configure different settings for each NP6 processor. The settings that you configure for an NP6 processor with the config system np6 command apply to traffic processed by all interfaces connected to that NP6 processor. This includes the physical interfaces connected to the NP6 processor as well as all subinterfaces, VLAN interfaces, IPsec interfaces, LAGs and so on associated with the physical interfaces connected to the NP6 processor.

```
config system np6
edit { name }
# Configure NP6 attributes.
set name { string } Device Name. size[31]
set fastpath { disable | enable } Enable/disable NP4 or NP6 offloading (also called fast path).
set low-latency-mode { disable | enable } Enable/disable low latency mode.
set per-session-accounting { disable | enable-by-log | all-enable } Enable/disable per-session accounting.
    disable Disable per-session accounting.
    enable-by-log Per-session accounting only for sessions with traffic logging enabled in firewall policy.
    all-enable Per-session accounting for all sessions.
set garbage-session-collector { disable | enable } Enable/disable garbage session collector.
set session-collector-interval { integer } Set garbage session collection cleanup interval (1 - 100 sec, default 64). range[1-100]
set session-timeout-interval { integer } Set session timeout interval (0 - 1000 sec, default 40 sec). range[0-1000]
set session-timeout-random-range { integer } Set the randomization range (0 - 1000 sec, default 8 sec). range[0-1000]
set session-timeout-fixed { disable | enable } Enable/disable fixed timeout interval mode.
set tcpsyn-max { integer } Maximum TCP SYN packet rate (10K - 4G pps, default = 5M pps). range[10000-4000000000]
set tcp-max { integer } Maximum TCP packet rate (10K - 4G pps, default = 5M pps). range[10000-4000000000]
set udp-max { integer } Maximum UDP packet rate (10K - 4G pps, default = 5M pps). range[10000-4000000000]
set icmp-max { integer } Maximum ICMP packet rate (10K - 4G pps, default = 1M pps). range[10000-4000000000]
set sctp-max { integer } Maximum SCTP packet rate (10K - 4G pps, default = 1M pps). range[10000-4000000000]
set esp-max { integer } Maximum ESP packet rate (10K - 4G pps, default = 1M pps). range[10000-4000000000]
set ip-frag-max { integer } Maximum fragmented IP packet rate (10K - 4G pps, default = 1M pps). range[10000-4000000000]
set ip-others-max { integer } Maximum IP packet rate for other packets (packet types that cannot be set with other options) (10G - 4G
pps, default = 1M pps). range[10000-4000000000]
set arp-max { integer } Maximum ARP packet rate (10K - 4G pps, default = 1M pps). range[10000-4000000000]
set l2-others-max { integer } Maximum L2 packet rate for L2 packets that are not ARP packets (10K - 4G pps, default = 1M pps). range
[10000-4000000000]
set enable-shaper { disable | enable } Enable/Disable NPU host protection engine (HPE) shaper.
set tcp-syn-fin { allow | drop | trap-to-host } TCP SYN flood SYN/FIN flag set anomalies.
    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.
set tcp-fin-noack { allow | drop | trap-to-host }  TCP SYN flood with FIN flag set without ACK setting anomalies.
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.
set tcp-fin-only { allow | drop | trap-to-host }  TCP SYN flood with only FIN flag set anomalies.
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.
set tcp-no-flag { allow | drop | trap-to-host }  TCP SYN flood with no flag set anomalies.
allow        Allow TCP packets without flag set to pass.
drop        Drop TCP packets without flag set.
trap-to-host Forward TCP packets without flag set to FortiOS.
set tcp-syn-data { allow | drop | trap-to-host }  TCP SYN flood packets with data anomalies.
allow        Allow TCP syn packets with data to pass.
drop        Drop TCP syn packets with data.
trap-to-host Forward TCP syn packets with data to FortiOS.
set tcp-winnuke { allow | drop | trap-to-host }  TCP WinNuke anomalies.
allow        Allow TCP packets winnuke attack to pass.
drop        Drop TCP packets winnuke attack.
trap-to-host Forward TCP packets winnuke attack to FortiOS.
set tcp-land { allow | drop | trap-to-host }  TCP land anomalies.
allow        Allow TCP land attack to pass.
drop        Drop TCP land attack.
trap-to-host Forward TCP land attack to FortiOS.
set udp-land { allow | drop | trap-to-host }  UDP land anomalies.
allow        Allow UDP land attack to pass.
drop        Drop UDP land attack.
trap-to-host Forward UDP land attack to FortiOS.
set icmp-land { allow | drop | trap-to-host }  ICMP land anomalies.
allow        Allow ICMP land attack to pass.
drop        Drop ICMP land attack.
trap-to-host Forward ICMP land attack to FortiOS.
set icmp-frag { allow | drop | trap-to-host }  Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.
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.
set ipv4-land { allow | drop | trap-to-host }  Land anomalies.
allow        Allow IPv4 land attack to pass.
drop        Drop IPv4 land attack.
trap-to-host Forward IPv4 land attack to FortiOS.
set ipv4-proto-err { allow | drop | trap-to-host }  Invalid layer 4 protocol anomalies.
```

```
    allow      Allow IPv4 invalid L4 protocol to pass.
    drop       Drop IPv4 invalid L4 protocol.
    trap-to-host Forward IPv4 invalid L4 protocol to FortiOS.
set ipv4-unknopt { allow | drop | trap-to-host } Unknown option anomalies.
    allow      Allow IPv4 with unknown options to pass.
    drop       Drop IPv4 with unknown options.
    trap-to-host Forward IPv4 with unknown options to FortiOS.
set ipv4-optrr { allow | drop | trap-to-host } Record route option anomalies.
    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.
set ipv4-optssrr { allow | drop | trap-to-host } Strict source record route option anomalies.
    allow      Allow IPv4 with strict source record route option to pass.
    drop       Drop IPv4 with strict source record route option.
    trap-to-host Forward IPv4 with strict source record route option to FortiOS.
set ipv4-optlsrr { allow | drop | trap-to-host } Loose source record route option anomalies.
    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.
set ipv4-optstream { allow | drop | trap-to-host } Stream option anomalies.
    allow      Allow IPv4 with stream option to pass.
    drop       Drop IPv4 with stream option.
    trap-to-host Forward IPv4 with stream option to FortiOS.
set ipv4-optsecurity { allow | drop | trap-to-host } Security option anomalies.
    allow      Allow IPv4 with security option to pass.
    drop       Drop IPv4 with security option.
    trap-to-host Forward IPv4 with security option to FortiOS.
set ipv4-opttimestamp { allow | drop | trap-to-host } Timestamp option anomalies.
    allow      Allow IPv4 with timestamp option to pass.
    drop       Drop IPv4 with timestamp option.
    trap-to-host Forward IPv4 with timestamp option to FortiOS.
set ipv4-csum-err { drop | trap-to-host } Invalid IPv4 IP checksum anomalies.
    drop       Drop IPv4 invalid IP checksum.
    trap-to-host Forward IPv4 invalid IP checksum to main CPU for processing.
set tcp-csum-err { drop | trap-to-host } Invalid IPv4 TCP checksum anomalies.
    drop       Drop IPv4 invalid TCP checksum.
    trap-to-host Forward IPv4 invalid TCP checksum to main CPU for processing.
set udp-csum-err { drop | trap-to-host } Invalid IPv4 UDP checksum anomalies.
    drop       Drop IPv4 invalid UDP checksum.
    trap-to-host Forward IPv4 invalid UDP checksum to main CPU for processing.
set icmp-csum-err { drop | trap-to-host } Invalid IPv4 ICMP checksum anomalies.
    drop       Drop IPv4 invalid ICMP checksum.
    trap-to-host Forward IPv4 invalid ICMP checksum to main CPU for processing.
```

```
set ipv6-land { allow | drop | trap-to-host } Land anomalies.
    allow      Allow IPv6 land attack to pass.
    drop       Drop IPv6 land attack.
    trap-to-host Forward IPv6 land attack to FortiOS.
set ipv6-proto-err { allow | drop | trap-to-host } Layer 4 invalid protocol anomalies.
    allow      Allow IPv6 L4 invalid protocol to pass.
    drop       Drop IPv6 L4 invalid protocol.
    trap-to-host Forward IPv6 L4 invalid protocol to FortiOS.
set ipv6-unknopt { allow | drop | trap-to-host } Unknown option anomalies.
    allow      Allow IPv6 with unknown options to pass.
    drop       Drop IPv6 with unknown options.
    trap-to-host Forward IPv6 with unknown options to FortiOS.
set ipv6-saddr-err { allow | drop | trap-to-host } Source address as multicast anomalies.
    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.
set ipv6-daddr-err { allow | drop | trap-to-host } Destination address as unspecified or loopback address anomalies.
    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.
set ipv6-optralert { allow | drop | trap-to-host } Router alert option anomalies.
    allow      Allow IPv6 with router alert option to pass.
    drop       Drop IPv6 with router alert option.
    trap-to-host Forward IPv6 with router alert option to FortiOS.
set ipv6-optjumbo { allow | drop | trap-to-host } Jumbo options anomalies.
    allow      Allow IPv6 with jumbo option to pass.
    drop       Drop IPv6 with jumbo option.
    trap-to-host Forward IPv6 with jumbo option to FortiOS.
set ipv6-opttunnel { allow | drop | trap-to-host } Tunnel encapsulation limit option anomalies.
    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.
set ipv6-opthomeaddr { allow | drop | trap-to-host } Home address option anomalies.
    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.
set ipv6-optnsap { allow | drop | trap-to-host } Network service access point address option anomalies.
    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.
set ipv6-optendpid { allow | drop | trap-to-host } End point identification anomalies.
    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.
set ipv6-optinvld { allow | drop | trap-to-host }  Invalid option anomalies.Invalid option anomalies.
        allow        Allow IPv6 with invalid option to pass.
        drop         Drop IPv6 with invalid option.
        trap-to-host  Forward IPv6 with invalid option to FortiOS.
    next
end
```

name {np6_0 | np6_1 |...}

Change the settings for one of the FortiGate unit's NP6 processors.

fastpath {disable | enable}

Enable fastpath acceleration to offload sessions to the NP6 processor. You can disable fastpath if you don't want the NP6 processor to offload sessions. Default enable.

per-session-accounting {all-enable | disable | enable-by-log}

Per-session accounting is a logging feature that allows the FortiGate to report the correct bytes/pkt numbers per session for sessions offloaded to an NP6 processor. This information appears in traffic log messages as well as in FortiView. When offloaded sessions appear on the FortiView All Sessions console they include an icon identifying them as NP sessions. You can hover over the NP icon to see some information about the offloaded sessions. By default, per-session accounting is set to `enable-by-log`, which results in per-session accounting being turned on when you enable traffic logging in a policy. You can disable per-session accounting or select `all-enable` to enable per-session accounting for all sessions whether or traffic logging is enabled or not. Per-session accounting can affect NP6 offloading performance. So you should only enable per-session accounting if you need the accounting information. Enabling per-session accounting only supports traffic log messages and does not provide traffic flow data for sFlow or NetFlow.

garbage-session-collector {disable | enable}

Enable deleting expired or garbage sessions. Disabled by default.

session-collector-interval <interval>

Set the expired or garbage session collector time interval in seconds. The range is 1 to 100 seconds. The default is 64 seconds.

session-timeout-interval <interval>

Set the timeout for inactive sessions. The range is 0 to 1000 seconds. The default is 40 seconds.

session-timeout-random-range <range>

Set the random timeout for inactive sessions. The range is 0 to 1000 seconds. The default is 8 seconds.

session-timeout-fixed {disable | enable}

Force session timeouts at fixed instead of random intervals. Disabled by default.

config fp-anomaly-v4

Configure how the NP6 processor does IPv4 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called `trap-to-host`). Selecting `trap-to-host` turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy but the anomaly protection is done by the CPU instead of the NP6.

tcp-syn-fin {allow | drop | trap-to-host}

Detect TCP SYN flood SYN/FIN flag set anomalies. Default is `allow`.

tcp-fin-noack {allow | drop | trap-to-host}

Detect TCP SYN flood with FIN flag set without ACK setting anomalies. Default is `trap-to-host`.

tcp-fin-only {allow | drop | trap-to-host}

Detect TCP SYN flood with only FIN flag set anomalies. Default is `trap-to-host`.

tcp-no-flag {allow | drop | trap-to-host}

Detect TCP SYN flood with no flag set anomalies. Default is `allow`.

tcp-syn-data {allow | drop | trap-to-host}

Detect TCP SYN flood packets with data anomalies. Default is `allow`.

tcp-winnuke {allow | drop | trap-to-host}

Detect TCP WinNuke anomalies. Default is `trap-to-host`.

tcp-land {allow | drop | trap-to-host}

Detect TCP land anomalies. Default is `trap-to-host`.

udp-land {allow | drop | trap-to-host}

Detect UDP land anomalies. Default is `trap-to-host`.

icmp-land {allow | drop | trap-to-host}

Detect ICMP land anomalies. Default is `trap-to-host`.

icmp-frag {allow | drop | trap-to-host}

Detect Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies. Default is `allow`.

ipv4-land {allow | drop | trap-to-host}

Detect IPv4 land anomalies. Default is `trap-to-host`.

ipv4-proto-err {allow | drop | trap-to-host}

Detect IPv4 invalid layer 4 protocol anomalies. Default is `trap-to-host`.

ipv4-unknopt {allow | drop | trap-to-host}

Detect IPv4 unknown option anomalies. Default is `trap-to-host`.

ipv4-optrr {allow | drop | trap-to-host}

Detect IPv4 record route option anomalies. Default is `trap-to-host`.

ipv4-optssrr {allow | drop | trap-to-host}

Detect IPv4 strict source record route option anomalies. Default is `trap-to-host`.

ipv4-optlsrr {allow | drop | trap-to-host}

Detect IPv4 loose source record route option anomalies. Default is `trap-to-host`.

ipv4-optstream {allow | drop | trap-to-host}

Detect IPv4 stream option anomalies.. Default is `trap-to-host`.

ipv4-optsecurity {allow | drop | trap-to-host}

Detect IPv4 security option anomalies. Default is `trap-to-host`.

ipv4-opttimestamp {allow | drop | trap-to-host}

Detect IPv4 timestamp option anomalies. Default is `trap-to-host`.

config fp-anomaly-v6

Configure how the NP6 processor does IPv6 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called “trap-to-host”). Selecting “trap-to-host” turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy.

ipv6-land {allow | drop | trap-to-host}

Detect IPv6 land anomalies. Default is `trap-to-host`.

ipv6-proto-err {allow | drop | trap-to-host}

Detect layer 4 invalid protocol anomalies. Default is `trap-to-host`.

ipv6-unknopt {allow | drop | trap-to-host}

Detect IPv6 unknown option anomalies. Default is `trap-to-host`.

ipv6-saddr-err {allow | drop | trap-to-host}

Detect source address as multicast anomalies. Default is `trap-to-host`.

ipv6-daddr-err {allow | drop | trap-to-host}

Detect IPv6 destination address as unspecified or loopback address anomalies. Default is `trap-to-host`.

ipv6-optralert {allow | drop | trap-to-host}

Detect IPv6 router alert option anomalies. Default is `trap-to-host`.

ipv6-optjumbo {allow | drop | trap-to-host}

Detect IPv6 jumbo options anomalies. Default is `trap-to-host`.

ipv6-opttunnel {allow | drop | trap-to-host}

Detect IPv6 tunnel encapsulation limit option anomalies. Default is `trap-to-host`.

ipv6-opthomeaddr {allow | drop | trap-to-host}

Detect IPv6 home address option anomalies. Default is `trap-to-host`.

ipv6-optnsap {allow | drop | trap-to-host}

Detect IPv6 network service access point address option anomalies. Default is `trap-to-host`.

ipv6-optendpid {allow | drop | trap-to-host}

Detect IPv6 end point identification anomalies. Default is `trap-to-host`.

ipv6-optinvld {allow | drop | trap-to-host}

Detect IPv6 invalid option anomalies. Default is `trap-to-host`.

system npu

Configure Network Processor (NP) options for FortiGates with NP6 and NP4 network processors.

```
config system npu
  set dedicated-management-cpu { enable | disable }  Enable to dedicate one CPU for GUI and CLI connections when NPs are busy.
  config port-cpu-map
    edit { interface }
      # Configure NPU interface to CPU core mapping.
      set interface { string }  The interface to map to a CPU core. size[15]
      set cpu-core { string }  The CPU core to map to an interface. size[31]
    next
  set capwap-offload { enable | disable }  Enable/disable offloading managed FortiAP and FortiLink CAPWAP sessions.
  set ipsec-enc-subengine-mask { string }  IPsec encryption subengine mask (0x1 - 0xff, default 0xff).
  set ipsec-dec-subengine-mask { string }  IPsec decryption subengine mask (0x1 - 0xff, default 0xff).
  set np6-cps-optimization-mode { enable | disable }  Enable/disable NP6 connection per second (CPS) optimization mode.
  set sw-np-bandwidth { option }  Bandwidth between NP and switch
    0G  Default value. No bandwidth control.
    2G  2Gbps.
    4G  4Gbps.
    5G  5Gbps.
    6G  6Gbps.
  set strip-esp-padding { enable | disable }  Enable/disable stripping ESP padding.
  set strip-clear-text-padding { enable | disable }  Enable/disable stripping clear text padding.
end
```

dedicated-management-cpu {disable | enable}

The GUI and CLI of FortiGate units with NP6 and NP4 processors may become unresponsive when the system is under heavy processing load because NP6 or NP4 interrupts overload the CPUs preventing CPU cycles from being used for management tasks. You can improve GUI and CLI performance in this situation by enabling this option to dedicate CPU core 0 to management tasks. All management tasks are then processed by CPU 0 and NP6 or NP4 interrupts are handled by the remaining CPU cores. Disabled by default.

capwap-offload {disable | enable}

Enable offloading managed FortiAP and FortiLink CAPWAP sessions to NP6 processors. Enabled by default.

{ipsec-dec-subengine-mask | ipsec-enc-subengine-mask} <engine-mask>

Use these commands to change the number of IPsec engines used for decryption and encryption. These settings are applied to all of the NP6 processors in the FortiGate unit. <engine-mask> is a hexadecimal number in the range 0x01 to 0xff where each bit represents one IPsec engine. The default <engine-mask> is 0xff which means all IPsec engines are used. Add a lower <engine-mask> to use fewer engines for decryption or encryption. NP6 processors use multiple IPsec engines to accelerate IPsec decryption and encryption. In some cases out of order ESP packets can cause problems if multiple IPsec engines are running. To resolve this problem you can configure all of the NP6 processors to use fewer IPsec engines. to use fewer engines for decryption or encryption. NP6 processors use multiple IPsec engines to accelerate IPsec decryption and encryption. In some cases out of order ESP packets can cause problems if multiple IPsec engines are running. To resolve this problem you can configure all of the NP6 processors to use fewer IPsec engines.

np6-cps-optimization-mode {disable | enable}

Enable to operate NP6s in a mode optimized for more connections per second (CPS). Disabled by default.

strip-esp-padding {disable | enable}

strip-clear-text-padding {disable | enable}

In some situations, when clear text or ESP packets in IPsec sessions may have large amounts of layer 2 padding, the NP6 IPsec engine may not be able to process them and the session may be blocked.

If you notice dropped IPsec sessions, you could try using the following CLI options to cause the NP6 processor to strip clear text padding and ESP padding before send the packets to the IPsec engine. With padding stripped, the session can be processed normally by the IPsec engine.

Use the following command to strip ESP padding:

```
config system npu
  set strip-esp-padding enable
  set strip-clear-text-padding enable
end
```

Stripping clear text and ESP padding are both disabled by default.

host-shortcut-mode {bi-directional | host-shortcut}

Due to NP6 internal packet buffer limitations, some offloaded packets received at a 10Gbps interface and destined for a 1Gbps interface can be dropped, reducing performance for TCP and IP tunnel traffic. If you experience this performance reduction, you can use the following command to disable offloading sessions passing from 10Gbps interfaces to 1Gbps interfaces:

```
config system npu
  set host-shortcut-mode host-shortcut
```

end

Select `host-shortcut` to stop offloading TCP and IP tunnel packets passing from 10Gbps interfaces to 1Gbps interfaces. TCP and IP tunnel packets passing from 1Gbps interfaces to 10Gbps interfaces are still offloaded as normal.

If `host-shortcut` is set to the default `bi-directional` setting, packets in both directions are offloaded.

This option is only available if your FortiGate has 10G and 1G interfaces accelerated by NP6 processors.

system ntp

Introduction.

```
config system ntp
  set ntpsync { enable | disable }  Enable/disable setting the FortiGate system time by synchronizing with an NTP Server.
  set type { fortiguard | custom }  Use the FortiGuard NTP server or any other available NTP Server.
    fortiguard  Use the FortiGuard NTP server.
    custom      Use any other available NTP server.
  set syncinterval { integer }  NTP synchronization interval (1 - 1440 min). range[1-1440]
config ntpserver
  edit { id }
    # Configure the FortiGate to connect to any available third-party NTP server.
    set id { integer }  NTP server ID. range[0-4294967295]
    set server { string }  IP address or hostname of the NTP Server. size[63]
    set ntpv3 { enable | disable }  Enable to use NTPv3 instead of NTPv4.
    set authentication { enable | disable }  Enable/disable MD5 authentication.
    set key { password_string }  Key for MD5 authentication. size[59]
    set key-id { integer }  Key ID for authentication. range[0-4294967295]
  next
  set source-ip { ipv4 address }  Source IP for communications to the NTP server.
  set server-mode { enable | disable }  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.
  config interface
    edit { interface-name }
      # FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services.
      set interface-name { string }  Interface name. size[64] - datasource(s): system.interface.name
    next
  end
```

system object-tag

Introduction.

```
config system object-tag
  edit { name }
  # Configure object tags.
  set name { string } Name of tag used throughout the configuration. size[63]
  next
end
```

system password-policy

Configure a password policy to be used for administrator accounts and/or IPsec VPN pre-shared keys.

```
config system password-policy
  set status { enable | disable }  Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.
  set apply-to { admin-password | ipsec-preshared-key }  Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.
    admin-password  Apply to administrator passwords.
    ipsec-preshared-key  Apply to IPsec pre-shared keys.
  set minimum-length { integer }  Minimum password length (8 - 128, default = 8). range[8-128]
  set min-lower-case-letter { integer }  Minimum number of lowercase characters in password (0 - 128, default = 0). range[0-128]
  set min-upper-case-letter { integer }  Minimum number of uppercase characters in password (0 - 128, default = 0). range[0-128]
  set min-non-alphanumeric { integer }  Minimum number of non-alphanumeric characters in password (0 - 128, default = 0). range[0-128]
  set min-number { integer }  Minimum number of numeric characters in password (0 - 128, default = 0). range[0-128]
  set change-4-characters { enable | disable }  Enable/disable requiring that at least 4 characters must be changed in a new password. (This attribute overrides reuse-password if both are enabled.)
  set expire-status { enable | disable }  Enable/disable password expiration.
  set expire-day { integer }  Number of days after which passwords expire (1 - 999 days, default = 90). range[1-999]
  set reuse-password { enable | disable }  Enable/disable reusing the same password when the old password expires. (if both reuse-password and change-4-characters are enabled, change-4-characters overrides.)
end
```

status {enable | disable}

Enable or disable enforcing a password policy. Disabled by default.

apply to {admin-password | ipsec-preshared-key}

Select which passwords must follow the policy. The options are the passwords for administrative accounts, IPsec VPN pre-shared keys, or both. The default is `admin-password`.

minimum-length <int>

Set the minimum number of characters required for a password. The default is 8.

min-lower-case-letter <int>

Set the minimum number of lower case letters that must be used in a password. The default is 0.

min-upper-case-letter <int>

Set the minimum number of upper case letters that must be used in a password. The default is 0.

min-non-alphanumeric <int>

Set the minimum number of non-alphanumeric characters that must be used in a password. The default is 0.

min-number <int>

Set the minimum number of numbers that must be used in a password. The default is 0.

change-4-characters {enable | disable}

Enable or disable to require a new password to differ from the old password by at least four characters. Disabled by default.

expire-status {enable | disable}

Enable or disable password expiration. Disabled by default.

expire-day <int>

Set the number of days after which a password expires. The default is 90. This option only appears when `expire-status` is enabled.

reuse-password {enable | disable}

Enable or disable allowing users to re-use a password. Enabled by default.

system password-policy-guest-admin

Introduction.

```
config system password-policy-guest-admin
    set status { enable | disable }  Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared
    keys.
    set apply-to { guest-admin-password }  Guest administrator to which this password policy applies.
        guest-admin-password  Apply to guest administrator password.
    set minimum-length { integer }  Minimum password length (8 - 128, default = 8). range[8-128]
    set min-lower-case-letter { integer }  Minimum number of lowercase characters in password (0 - 128, default = 0). range[0-128]
    set min-upper-case-letter { integer }  Minimum number of uppercase characters in password (0 - 128, default = 0). range[0-128]
    set min-non-alphanumeric { integer }  Minimum number of non-alphanumeric characters in password (0 - 128, default = 0). range[0-128]
    set min-number { integer }  Minimum number of numeric characters in password (0 - 128, default = 0). range[0-128]
    set change-4-characters { enable | disable }  Enable/disable requiring that at least 4 characters must be changed in a new password. (This
attribute overrides reuse-password if both are enabled.)
    set expire-status { enable | disable }  Enable/disable password expiration.
    set expire-day { integer }  Number of days after which passwords expire (1 - 999 days, default = 90). range[1-999]
    set reuse-password { enable | disable }  Enable/disable reusing the same password when the old password expires. (if both reuse-password and
change-4-characters are enabled, change-4-characters overrides.)
end
```

system physical-switch

Introduction.

```
config system physical-switch
  edit { name }
  # Configure physical switches.
  set age-enable { enable | disable }  Enable/disable layer 2 age timer.
  config port
    edit { name }
    # Configure member ports.
    set speed { option }  Speed.
      auto      Automatically adjust speed.
      10full    10M full-duplex.
      10half    10M half-duplex.
      100full   100M full-duplex.
      100half   100M half-duplex.
      1000full  1000M full-duplex.
      1000half  1000M half-duplex.
      1000auto  1000M auto adjust.
    set status { up | down }  Interface status.
      up      Interface up.
      down    Interface down.
    set name { string }  Physical port name. size[15]
  next
  set age-val { integer }  Layer 2 table age timer Value. range[0-4294967295]
  set name { string }  Name. size[15]
next
end
```

system pppoe-interface

Introduction.

```
config system pppoe-interface
  edit { name }
  # Configure the PPPoE interfaces.
  set name { string } Name of the PPPoE interface. size[15]
  set dial-on-demand { enable | disable } Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE
interface.
  set ipv6 { enable | disable } Enable/disable IPv6 Control Protocol (IPv6CP).
  set device { string } Name for the physical interface. size[15] - datasource(s): system.interface.name
  set username { string } User name. size[64]
  set password { password_string } Enter the password. size[128]
  set auth-type { option } PPP authentication type to use.
    auto Automatically choose the authentication method.
    pap PAP authentication.
    chap CHAP authentication.
    mschapv1 MS-CHAPv1 authentication.
    mschapv2 MS-CHAPv2 authentication.
  set ipunnumbered { ipv4 address } PPPoE unnumbered IP.
  set pppoe-unnumbered-negotiate { enable | disable } Enable/disable PPPoE unnumbered negotiation.
  set idle-timeout { integer } PPPoE auto disconnect after idle timeout (0-4294967295 sec). range[0-4294967295]
  set disc-retry-timeout { integer } PPPoE discovery init timeout value in (0-4294967295 sec). range[0-4294967295]
  set padt-retry-timeout { integer } PPPoE terminate timeout value in (0-4294967295 sec). range[0-4294967295]
  set service-name { string } PPPoE service name. size[63]
  set ac-name { string } PPPoE AC name. size[63]
  set lcp-echo-interval { integer } PPPoE LCP echo interval in (0-4294967295 sec, default = 5). range[0-4294967295]
  set lcp-max-echo-fails { integer } Maximum missed LCP echo messages before disconnect (0-4294967295, default = 3). range[0-4294967295]
  next
end
```

system probe-response

Introduction.

```
config system probe-response
  set port { integer }   Port number to response. range[1-65535]
  set http-probe-value { string }   Value to respond to the monitoring server. size[1024]
  set ttl-mode { reinit | decrease | retain }   Mode for TWAMP packet TTL modification.
    reinit   Reinitialize TTL.
    decrease Decrease TTL.
    retain   Retain TTL.
  set mode { none | http-probe | twamp }   SLA response mode.
    none     Disable probe.
    http-probe HTTP probe.
    twamp    Two way active measurement protocol.
  set security-mode { none | authentication }   Twamp responder security mode.
    none     Unauthenticated mode.
    authentication Authenticated mode.
  set password { password_string }   Twamp responder password in authentication mode size[128]
  set timeout { integer }   An inactivity timer for a twamp test session. range[10-3600]
end
```

system proxy-arp

Introduction.

```
config system proxy-arp
  edit { id }
  # Configure proxy-ARP.
  set id { integer } Unique integer ID of the entry. range[0-4294967295]
  set interface { string } Interface acting proxy-ARP. size[15] - datasource(s): system.interface.name
  set ip { ipv4 address } IP address or start IP to be proxied.
  set end-ip { ipv4 address } End IP of IP range to be proxied.
next
end
```

system replacemsg admin

Introduction.

```
config system replacemsg admin
  edit { msg-type }
    # Replacement messages.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
      none No header type.
      http HTTP
      8bit 8 bit.
    set format { none | text | html } Format flag.
      none No format type.
      text Text format.
      html HTML format.
  next
end
```

system replacemsg alertmail

Introduction.

```
config system replacemsg alertmail
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg auth

Introduction.

```
config system replacemsg auth
edit { msg-type }
# Replacement messages.
set msg-type { string } Message type. size[28]
set buffer { string } Message string. size[32768]
set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
end
```


system replacemsg device-detection-portal

Introduction.

```
config system replacemsg device-detection-portal
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg ec

Introduction.

```
config system replacemsg ec
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg fortiguard-wf

Introduction.

```
config system replacemsg fortiguard-wf
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg ftp

Introduction.

```
config system replacemsg ftp
edit { msg-type }
# Replacement messages.
set msg-type { string } Message type. size[28]
set buffer { string } Message string. size[32768]
set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
end
```

system replacemsg http

Introduction.

```
config system replacemsg http
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg mail

Introduction.

```
config system replacemsg mail
  edit { msg-type }
    # Replacement messages.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
      none No header type.
      http HTTP
      8bit 8 bit.
    set format { none | text | html } Format flag.
      none No format type.
      text Text format.
      html HTML format.
  next
end
```

system replacemsg nac-quar

Introduction.

```
config system replacemsg nac-quar
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg nntp

Introduction.

```
config system replacemsg nntp
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```


system replacemsg spam

Introduction.

```
config system replacemsg spam
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg sslvpn

Introduction.

```
config system replacemsg sslvpn
  edit { msg-type }
    # Replacement messages.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
      none No header type.
      http HTTP
      8bit 8 bit.
    set format { none | text | html } Format flag.
      none No format type.
      text Text format.
      html HTML format.
  next
end
```

system replacemsg traffic-quota

Introduction.

```
config system replacemsg traffic-quota
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg utm

Introduction.

```
config system replacemsg utm
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg webproxy

Introduction.

```
config system replacemsg webproxy
  edit { msg-type }
  # Replacement messages.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
end
```

system replacemsg-group

Introduction.

```
config system replacemsg-group
  edit { name }
  # Configure replacement message groups.
  set name { string }  Group name. size[35]
  set comment { string }  Comment. size[255]
  set group-type { default | utm | auth | ec }  Group type.
    default  Per-vdom replacement messages.
    utm      For use with UTM settings in firewall policies.
    auth     For use with authentication pages in firewall policies.
    ec       For use with endpoint-control profiles.
config mail
  edit { msg-type }
  # Replacement message table entries.
  set msg-type { string }  Message type. size[28]
  set buffer { string }  Message string. size[32768]
  set header { none | http | 8bit }  Header flag.
    none  No header type.
    http  HTTP
    8bit  8 bit.
  set format { none | text | html }  Format flag.
    none  No format type.
    text  Text format.
    html  HTML format.
  next
config http
  edit { msg-type }
  # Replacement message table entries.
  set msg-type { string }  Message type. size[28]
  set buffer { string }  Message string. size[32768]
  set header { none | http | 8bit }  Header flag.
    none  No header type.
    http  HTTP
    8bit  8 bit.
  set format { none | text | html }  Format flag.
    none  No format type.
```

```
        text Text format.
        html HTML format.
    next
config webproxy
edit { msg-type }
# Replacement message table entries.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
        none No header type.
        http HTTP
        8bit 8 bit.
    set format { none | text | html } Format flag.
        none No format type.
        text Text format.
        html HTML format.
    next
config ftp
edit { msg-type }
# Replacement message table entries.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
        none No header type.
        http HTTP
        8bit 8 bit.
    set format { none | text | html } Format flag.
        none No format type.
        text Text format.
        html HTML format.
    next
config nntp
edit { msg-type }
# Replacement message table entries.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
        none No header type.
        http HTTP
        8bit 8 bit.
    set format { none | text | html } Format flag.
        none No format type.
        text Text format.
```

```
        html HTML format.
    next
config fortiguard-wf
edit { msg-type }
# Replacement message table entries.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
        none No header type.
        http HTTP
        8bit 8 bit.
    set format { none | text | html } Format flag.
        none No format type.
        text Text format.
        html HTML format.
    next
config spam
edit { msg-type }
# Replacement message table entries.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
        none No header type.
        http HTTP
        8bit 8 bit.
    set format { none | text | html } Format flag.
        none No format type.
        text Text format.
        html HTML format.
    next
config alertmail
edit { msg-type }
# Replacement message table entries.
    set msg-type { string } Message type. size[28]
    set buffer { string } Message string. size[32768]
    set header { none | http | 8bit } Header flag.
        none No header type.
        http HTTP
        8bit 8 bit.
    set format { none | text | html } Format flag.
        none No format type.
        text Text format.
        html HTML format.
```



```
next
config admin
edit { msg-type }
# Replacement message table entries.
set msg-type { string } Message type. size[28]
set buffer { string } Message string. size[32768]
set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
config auth
edit { msg-type }
# Replacement message table entries.
set msg-type { string } Message type. size[28]
set buffer { string } Message string. size[32768]
set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
config sslvpn
edit { msg-type }
# Replacement message table entries.
set msg-type { string } Message type. size[28]
set buffer { string } Message string. size[32768]
set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
```

```
config ec
  edit { msg-type }
  # Replacement message table entries.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
config device-detection-portal
  edit { msg-type }
  # Replacement message table entries.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
config nac-quar
  edit { msg-type }
  # Replacement message table entries.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
  next
config traffic-quota
```

```
edit { msg-type }
# Replacement message table entries.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
config utm
edit { msg-type }
# Replacement message table entries.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
config custom-message
edit { msg-type }
# Replacement message table entries.
  set msg-type { string } Message type. size[28]
  set buffer { string } Message string. size[32768]
  set header { none | http | 8bit } Header flag.
    none No header type.
    http HTTP
    8bit 8 bit.
  set format { none | text | html } Format flag.
    none No format type.
    text Text format.
    html HTML format.
next
end
```


system replacemsg-image

Introduction.

```
config system replacemsg-image
  edit { name }
  # Configure replacement message images.
  set name { string } Image name. size[23]
  set image-type { gif | jpg | tiff | png } Image type.
    gif GIF image.
    jpg JPEG image.
    tiff TIFF image.
    png PNG image.
  set image-base64 { string } Image data. size[32768]
next
end
```

system resource-limits

Introduction.

```
config system resource-limits
  set session { integer }    Maximum number of sessions. range[0-4294967295]
  set ipsec-phase1 { integer } Maximum number of VPN IPsec phase1 tunnels. range[0-4294967295]
  set ipsec-phase2 { integer } Maximum number of VPN IPsec phase2 tunnels. range[0-4294967295]
  set dialup-tunnel { integer } Maximum number of dial-up tunnels. range[0-4294967295]
  set firewall-policy { integer } Maximum number of firewall policies. range[0-4294967295]
  set firewall-address { integer } Maximum number of firewall addresses. range[0-4294967295]
  set firewall-addrgrp { integer } Maximum number of firewall address groups. range[0-4294967295]
  set custom-service { integer } Maximum number of firewall custom services. range[0-4294967295]
  set service-group { integer } Maximum number of firewall service groups. range[0-4294967295]
  set onetime-schedule { integer } Maximum number of firewall one-time schedules. range[0-4294967295]
  set recurring-schedule { integer } Maximum number of firewall recurring schedules. range[0-4294967295]
  set user { integer } Maximum number of local users. range[0-4294967295]
  set user-group { integer } Maximum number of user groups. range[0-4294967295]
  set sslvpn { integer } Maximum number of SSL-VPN. range[0-4294967295]
  set proxy { integer } Maximum number of concurrent proxy users. range[0-4294967295]
  set log-disk-quota { integer } Log disk quota in MB. range[0-4294967295]
end
```

system session-helper

Introduction.

```
config system session-helper
  edit { id }
  # Configure session helper.
  set id { integer }   Session helper ID. range[0-4294967295]
  set name { option }  Helper name.
    ftp      FTP.
    tftp     TFTP.
    ras      RAS.
    h323     H323.
    tns      TNS.
    mms      MMS.
    sip      SIP.
    pptp     PPTP.
    rtsp     RTSP.
    dns-udp  DNS UDP.
    dns-tcp  DNS TCP.
    pmap     EMAP.
    rsh      RSH.
    dcerpc   DCERPC.
    mgcp     MGCP.
  set protocol { integer } Protocol number. range[0-255]
  set port { integer }   Protocol port. range[1-65535]
next
end
```

system session-ttl

Introduction.

```
config system session-ttl
  set default { string } Default timeout.
  config port
    edit { id }
      # Session TTL port.
      set id { integer } Table entry ID. range[0-65535]
      set protocol { integer } Protocol (0 - 255). range[0-255]
      set start-port { integer } Start port number. range[0-65535]
      set end-port { integer } End port number. range[0-65535]
      set timeout { string } Session timeout (TTL).
    next
  end
```


system settings

Introduction.

```
config system settings
  set comments { string }   VDOM comments. size[255]
  set opmode { nat | transparent }   Firewall operation mode (NAT or Transparent).
    nat           Change to NAT mode.
    transparent   Change to transparent mode.
  set inspection-mode { proxy | flow }   Inspection mode (proxy-based or flow-based).
    proxy         Proxy-based inspection.
    flow          Flow-based inspection.
  set ngfw-mode { profile-based | policy-based }   Next Generation Firewall (NGFW) mode.
    profile-based Application and web-filtering are configured using profiles applied to policy entries.
    policy-based  Application and web-filtering are configured as policy match conditions.
  set ssl-ssh-profile { string }   Profile for SSL/SSH inspection. size[35] - datasource(s): firewall.ssl-ssh-profile.name
  set http-external-dest { fortiweb | forticache }   Offload HTTP traffic to FortiWeb or FortiCache.
    fortiweb     Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.
    forticache   Offload HTTP traffic to FortiCache for external web caching and WAN optimization.
  set firewall-session-dirty { check-all | check-new | check-policy-option }   Select how to manage sessions affected by firewall policy configuration changes.
    check-all   All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.
    check-new    Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.
    check-policy-option Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.
  set manageip { string }   Transparent mode IPv4 management IP address and netmask.
  set gateway { ipv4 address }   Transparent mode IPv4 default gateway IP address.
  set ip { ipv4 classnet host }   IP address and netmask.
  set manageip6 { ipv6 prefix }   Transparent mode IPv6 management IP address and netmask.
  set gateway6 { ipv6 address }   Transparent mode IPv4 default gateway IP address.
  set ip6 { ipv6 prefix }   IPv6 address prefix for NAT mode.
  set device { string }   Interface to use for management access for NAT mode. size[35] - datasource(s): system.interface.name
  set bfd { enable | disable }   Enable/disable Bi-directional Forwarding Detection (BFD) on all interfaces.
  set bfd-desired-min-tx { integer }   BFD desired minimal transmit interval (1 - 100000 ms, default = 50). range[1-100000]
  set bfd-required-min-rx { integer }   BFD required minimal receive interval (1 - 100000 ms, default = 50). range[1-100000]
  set bfd-detect-mult { integer }   BFD detection multiplier (1 - 50, default = 3). range[1-50]
  set bfd-dont-enforce-src-port { enable | disable }   Enable to not enforce verifying the source port of BFD Packets.
  set utf8-spam-tagging { enable | disable }   Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.
```

```
set wccp-cache-engine { enable | disable } Enable/disable WCCP cache engine.
set vpn-stats-log { ipsec | pptp | l2tp | ssl } Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a
space.
    ipsec IPsec.
    pptp PPTP.
    l2tp L2TP.
    ssl SSL.
set vpn-stats-period { integer } Period to send VPN log statistics (60 - 86400 sec). range[60-86400]
set v4-ecmp-mode { source-ip-based | weight-based | usage-based | source-dest-ip-based } IPv4 Equal-cost multi-path (ECMP) routing and load bal-
ancing mode.
    source-ip-based Select next hop based on source IP.
    weight-based Select next hop based on weight.
    usage-based Select next hop based on usage.
    source-dest-ip-based Select next hop based on both source and destination IPs.
set mac-ttl { integer } Duration of MAC addresses in Transparent mode (300 - 8640000 sec, default = 300). range[300-8640000]
set fw-session-hairpin { enable | disable } Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiGate.
set snat-hairpin-traffic { enable | disable } Enable/disable source NAT (SNAT) for hairpin traffic.
set dhcp-proxy { enable | disable } Enable/disable the DHCP Proxy.
set dhcp-server-ip { string } DHCP Server IPv4 address.
set dhcp6-server-ip { string } DHCPv6 server IPv6 address.
set central-nat { enable | disable } Enable/disable central NAT.
config gui-default-policy-columns
    edit { name }
        # Default columns to display for policy lists on GUI.
        set name { string } Select column name. size[64]
    next
set lldp-transmission { enable | disable | global } Enable/disable Link Layer Discovery Protocol (LLDP) for this VDOM or apply global settings
to this VDOM.
set asymroute { enable | disable } Enable/disable IPv4 asymmetric routing.
set asymroute-icmp { enable | disable } Enable/disable ICMP asymmetric routing.
set tcp-session-without-syn { enable | disable } Enable/disable allowing TCP session without SYN flags.
set ses-denied-traffic { enable | disable } Enable/disable including denied session in the session table.
set strict-src-check { enable | disable } Enable/disable strict source verification.
set asymroute6 { enable | disable } Enable/disable asymmetric IPv6 routing.
set asymroute6-icmp { enable | disable } Enable/disable asymmetric ICMPv6 routing.
set sip-helper { enable | disable } Enable/disable the SIP session helper to process SIP sessions unless SIP sessions are accepted by the SIP
application layer gateway (ALG).
set sip-nat-trace { enable | disable } Enable/disable recording the original SIP source IP address when NAT is used.
set status { enable | disable } Enable/disable this VDOM.
set sip-tcp-port { integer } TCP port the SIP proxy monitors for SIP traffic (0 - 65535, default = 5060). range[1-65535]
set sip-udp-port { integer } UDP port the SIP proxy monitors for SIP traffic (0 - 65535, default = 5060). range[1-65535]
set sip-ssl-port { integer } TCP port the SIP proxy monitors for SIP SSL/TLS traffic (0 - 65535, default = 5061). range[0-65535]
set sccp-port { integer } TCP port the SCCP proxy monitors for SCCP traffic (0 - 65535, default = 2000). range[0-65535]
```

```
set multicast-forward { enable | disable } Enable/disable multicast forwarding.
set multicast-ttl-notchange { enable | disable } Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.
set multicast-skip-policy { enable | disable } Enable/disable allowing multicast traffic through the FortiGate without a policy check.
set allow-subnet-overlap { enable | disable } Enable/disable allowing interface subnets to use overlapping IP addresses.
set deny-tcp-with-icmp { enable | disable } Enable/disable denying TCP by sending an ICMP communication prohibited packet.
set ecmp-max-paths { integer } Maximum number of Equal Cost Multi-Path (ECMP) next-hops. Set to 1 to disable ECMP routing (1 - 100, default = 10). range[1-100]
set discovered-device-timeout { integer } Timeout for discovered devices (1 - 365 days, default = 28). range[1-365]
set email-portal-check-dns { disable | enable } Enable/disable using DNS to validate email addresses collected by a captive portal.
set default-voip-alg-mode { proxy-based | kernel-helper-based } Configure how the FortiGate handles VoIP traffic when a policy that accepts the traffic doesn't include a VoIP profile.
    proxy-based Use a default proxy-based VoIP ALG.
    kernel-helper-based Use the SIP session helper.
set gui-icap { enable | disable } Enable/disable ICAP on the GUI.
set gui-nat46-64 { enable | disable } Enable/disable NAT46 and NAT64 settings on the GUI.
set gui-implicit-policy { enable | disable } Enable/disable implicit firewall policies on the GUI.
set gui-dns-database { enable | disable } Enable/disable DNS database settings on the GUI.
set gui-load-balance { enable | disable } Enable/disable server load balancing on the GUI.
set gui-multicast-policy { enable | disable } Enable/disable multicast firewall policies on the GUI.
set gui-dos-policy { enable | disable } Enable/disable DoS policies on the GUI.
set gui-object-colors { enable | disable } Enable/disable object colors on the GUI.
set gui-replacement-message-groups { enable | disable } Enable/disable replacement message groups on the GUI.
set gui-voip-profile { enable | disable } Enable/disable VoIP profiles on the GUI.
set gui-ap-profile { enable | disable } Enable/disable FortiAP profiles on the GUI.
set gui-dynamic-profile-display { enable | disable } Enable/disable RADIUS Single Sign On (RSSO) on the GUI.
set gui-local-in-policy { enable | disable } Enable/disable Local-In policies on the GUI.
set gui-local-reports { enable | disable } Enable/disable local reports on the GUI.
set gui-wanopt-cache { enable | disable } Enable/disable WAN Optimization and Web Caching on the GUI.
set gui-explicit-proxy { enable | disable } Enable/disable the explicit proxy on the GUI.
set gui-dynamic-routing { enable | disable } Enable/disable dynamic routing on the GUI.
set gui-dlp { enable | disable } Enable/disable DLP on the GUI.
set gui-sslvpn-personal-bookmarks { enable | disable } Enable/disable SSL-VPN personal bookmark management on the GUI.
set gui-sslvpn-realms { enable | disable } Enable/disable SSL-VPN realms on the GUI.
set gui-policy-based-ipsec { enable | disable } Enable/disable policy-based IPsec VPN on the GUI.
set gui-threat-weight { enable | disable } Enable/disable threat weight on the GUI.
set gui-multiple-utm-profiles { enable | disable } Enable/disable multiple UTM profiles on the GUI.
set gui-spamfilter { enable | disable } Enable/disable Antispam on the GUI.
set gui-application-control { enable | disable } Enable/disable application control on the GUI.
set gui-ips { enable | disable } Enable/disable IPS on the GUI.
set gui-endpoint-control { enable | disable } Enable/disable endpoint control on the GUI.
set gui-endpoint-control-advanced { enable | disable } Enable/disable advanced endpoint control options on the GUI.
set gui-dhcp-advanced { enable | disable } Enable/disable advanced DHCP options on the GUI.
set gui-vpn { enable | disable } Enable/disable VPN tunnels on the GUI.
```

```
set gui-wireless-controller { enable | disable } Enable/disable the wireless controller on the GUI.
set gui-switch-controller { enable | disable } Enable/disable the switch controller on the GUI.
set gui-fortiap-split-tunneling { enable | disable } Enable/disable FortiAP split tunneling on the GUI.
set gui-webfilter-advanced { enable | disable } Enable/disable advanced web filtering on the GUI.
set gui-traffic-shaping { enable | disable } Enable/disable traffic shaping on the GUI.
set gui-wan-load-balancing { enable | disable } Enable/disable SD-WAN on the GUI.
set gui-antivirus { enable | disable } Enable/disable AntiVirus on the GUI.
set gui-webfilter { enable | disable } Enable/disable Web filtering on the GUI.
set gui-dnsfilter { enable | disable } Enable/disable DNS Filtering on the GUI.
set gui-waf-profile { enable | disable } Enable/disable Web Application Firewall on the GUI.
set gui-fortiextender-controller { enable | disable } Enable/disable FortiExtender on the GUI.
set gui-advanced-policy { enable | disable } Enable/disable advanced policy configuration on the GUI.
set gui-allow-unnamed-policy { enable | disable } Enable/disable the requirement for policy naming on the GUI.
set gui-email-collection { enable | disable } Enable/disable email collection on the GUI.
set gui-domain-ip-reputation { enable | disable } Enable/disable Domain and IP Reputation on the GUI.
set gui-multiple-interface-policy { enable | disable } Enable/disable adding multiple interfaces to a policy on the GUI.
set gui-policy-learning { enable | disable } Enable/disable firewall policy learning mode on the GUI.
set compliance-check { enable | disable } Enable/disable PCI DSS compliance checking.
set ike-session-resume { enable | disable } Enable/disable IKEv2 session resumption (RFC 5723).
set ike-quick-crash-detect { enable | disable } Enable/disable IKE quick crash detection (RFC 6290).
set ike-dn-format { with-space | no-space } Configure IKE ASN.1 Distinguished Name format conventions.
    with-space Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.
    no-space Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.
set block-land-attack { disable | enable } Enable/disable blocking of land attacks.
end
```

system sflow

Introduction.

```
config system sflow
    set collector-ip { ipv4 address }    IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to
    (default = 0.0.0.0).
    set collector-port { integer }    UDP port number used for sending sFlow datagrams (configure only if required by your sFlow collector or your net-
work configuration) (0 - 65535, default = 6343). range[0-65535]
    set source-ip { ipv4 address }    Source IP address for sFlow agent.
end
```

system sit-tunnel

Introduction.

```
config system sit-tunnel
  edit { name }
  # Configure IPv6 tunnel over IPv4.
  set name { string } Tunnel name. size[15]
  set source { ipv4 address } Source IP address of the tunnel.
  set destination { ipv4 address } Destination IP address of the tunnel.
  set ip6 { ipv6 prefix } IPv6 address of the tunnel.
  set interface { string } Interface name. size[15] - datasource(s): system.interface.name
  set auto-asic-offload { enable | disable } Enable/disable tunnel ASIC offloading.
next
end
```

system sms-server

Configure a cellphone service provider to send SMS text messages as part of two-factor authentication.

```
config system sms-server
  edit { name }
  # Configure SMS server for sending SMS messages to support user authentication.
  set name { string } Name of SMS server. size[35]
  set mail-server { string } Email-to-SMS server domain name. size[63]
  next
end
```

mail-server <server_name>

Set the domain name of the email-to-SMS server.

system snmp community

Introduction.

```
config system snmp community
  edit { id }
  # SNMP community configuration.
  set id { integer } Community ID. range[0-4294967295]
  set name { string } Community name. size[35]
  set status { enable | disable } Enable/disable this SNMP community.
config hosts
  edit { id }
  # Configure IPv4 SNMP managers (hosts).
  set id { integer } Host entry ID. range[0-4294967295]
  set source-ip { ipv4 address } Source IPv4 address for SNMP traps.
  set ip { string } IPv4 address of the SNMP manager (host).
  set ha-direct { enable | disable } Enable/disable direct management of HA cluster members.
  set host-type { any | query | trap } Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.
    any Accept queries from and send traps to this SNMP manager.
    query Accept queries from this SNMP manager but do not send traps.
    trap Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.
  next
config hosts6
  edit { id }
  # Configure IPv6 SNMP managers.
  set id { integer } Host6 entry ID. range[0-4294967295]
  set source-ipv6 { ipv6 address } Source IPv6 address for SNMP traps.
  set ipv6 { ipv6 prefix } SNMP manager IPv6 address prefix.
  set ha-direct { enable | disable } Enable/disable direct management of HA cluster members.
  set host-type { any | query | trap } Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.
    any Accept queries from and send traps to this SNMP manager.
    query Accept queries from this SNMP manager but do not send traps.
    trap Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.
  next
set query-v1-status { enable | disable } Enable/disable SNMP v1 queries.
set query-v1-port { integer } SNMP v1 query port (default = 161). range[1-65535]
set query-v2c-status { enable | disable } Enable/disable SNMP v2c queries.
set query-v2c-port { integer } SNMP v2c query port (default = 161). range[0-65535]
set trap-v1-status { enable | disable } Enable/disable SNMP v1 traps.
```



```

set trap-v1-lport { integer }   SNMP v1 trap local port (default = 162). range[1-65535]
set trap-v1-rport { integer }   SNMP v1 trap remote port (default = 162). range[1-65535]
set trap-v2c-status { enable | disable }   Enable/disable SNMP v2c traps.
set trap-v2c-lport { integer }   SNMP v2c trap local port (default = 162). range[1-65535]
set trap-v2c-rport { integer }   SNMP v2c trap remote port (default = 162). range[1-65535]
set events { option }   SNMP trap events.
    cpu-high                Send a trap when CPU usage is high.
    mem-low                 Send a trap when available memory is low.
    log-full               Send a trap when log disk space becomes low.
    intf-ip               Send a trap when an interface IP address is changed.
    vpn-tun-up            Send a trap when a VPN tunnel comes up.
    vpn-tun-down         Send a trap when a VPN tunnel goes down.
    ha-switch             Send a trap after an HA failover when the backup unit has taken over.
    ha-hb-failure         Send a trap when HA heartbeats are not received.
    ips-signature         Send a trap when IPS detects an attack.
    ips-anomaly           Send a trap when IPS finds an anomaly.
    av-virus              Send a trap when AntiVirus finds a virus.
    av-oversize           Send a trap when AntiVirus finds an oversized file.
    av-pattern            Send a trap when AntiVirus finds file matching pattern.
    av-fragmented        Send a trap when AntiVirus finds a fragmented file.
    fm-if-change          Send a trap when FortiManager interface changes. Send a FortiManager trap.
    fm-conf-change        Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
    bgp-established       Send a trap when a BGP FSM transitions to the established state.
    bgp-backward-transition Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
    ha-member-up          Send a trap when an HA cluster member goes up.
    ha-member-down        Send a trap when an HA cluster member goes down.
    ent-conf-change       Send a trap when an entity MIB change occurs (RFC4133).
    av-conserve           Send a trap when the FortiGate enters conserve mode.
    av-bypass             Send a trap when the FortiGate enters bypass mode.
    av-oversize-passed    Send a trap when AntiVirus passes an oversized file.
    av-oversize-blocked   Send a trap when AntiVirus blocks an oversized file.
    ips-pkg-update        Send a trap when the IPS signature database or engine is updated.
    ips-fail-open         Send a trap when the IPS network buffer is full.
    temperature-high      Send a trap when a temperature sensor registers a temperature that is too high.
    voltage-alert         Send a trap when a voltage sensor registers a voltage that is outside of the normal range.
    power-supply-failure  Send a trap when a power supply fails.
    faz-disconnect        Send a trap when a FortiAnalyzer disconnects from the FortiGate.
    fan-failure           Send a trap when a fan fails.
    wc-ap-up              Send a trap when a managed FortiAP comes up.
    wc-ap-down            Send a trap when a managed FortiAP goes down.
    fswctl-session-up     Send a trap when a FortiSwitch controller session comes up.
    fswctl-session-down   Send a trap when a FortiSwitch controller session goes down.

```

```
        load-balance-real-server-down Send a trap when a server load balance real server goes down.
        device-new                    Send a trap when a new device is found.
        per-cpu-high                  Send a trap when per-CPU usage is high.
    next
end
```

system snmp sysinfo

Introduction.

```
config system snmp sysinfo
  set status { enable | disable }  Enable/disable SNMP.
  set engine-id { string }  Local SNMP engineID string (maximum 24 characters). size[24]
  set description { string }  System description. size[255]
  set contact-info { string }  Contact information. size[255]
  set location { string }  System location. size[255]
  set trap-high-cpu-threshold { integer }  CPU usage when trap is sent. range[1-100]
  set trap-low-memory-threshold { integer }  Memory usage when trap is sent. range[1-100]
  set trap-log-full-threshold { integer }  Log disk usage when trap is sent. range[1-100]
end
```

system snmp user

Introduction.

```

config system snmp user
  edit { name }
  # SNMP user configuration.
  set name { string }   SNMP user name. size[32]
  set status { enable | disable }   Enable/disable this SNMP user.
  set trap-status { enable | disable }   Enable/disable traps for this SNMP user.
  set trap-lport { integer }   SNMPv3 local trap port (default = 162). range[0-65535]
  set trap-rport { integer }   SNMPv3 trap remote port (default = 162). range[0-65535]
  set queries { enable | disable }   Enable/disable SNMP queries for this user.
  set query-port { integer }   SNMPv3 query port (default = 161). range[0-65535]
  set notify-hosts { ipv4 address }   SNMP managers to send notifications (traps) to.
  set notify-hosts6 { ipv6 address }   IPv6 SNMP managers to send notifications (traps) to.
  set source-ip { ipv4 address }   Source IP for SNMP trap.
  set source-ipv6 { ipv6 address }   Source IPv6 for SNMP trap.
  set ha-direct { enable | disable }   Enable/disable direct management of HA cluster members.
  set events { option }   SNMP notifications (traps) to send.
    cpu-high           Send a trap when CPU usage is high.
    mem-low            Send a trap when available memory is low.
    log-full           Send a trap when log disk space becomes low.
    intf-ip            Send a trap when an interface IP address is changed.
    vpn-tun-up         Send a trap when a VPN tunnel comes up.
    vpn-tun-down       Send a trap when a VPN tunnel goes down.
    ha-switch          Send a trap after an HA failover when the backup unit has taken over.
    ha-hb-failure      Send a trap when HA heartbeats are not received.
    ips-signature       Send a trap when IPS detects an attack.
    ips-anomaly         Send a trap when IPS finds an anomaly.
    av-virus            Send a trap when AntiVirus finds a virus.
    av-oversize         Send a trap when AntiVirus finds an oversized file.
    av-pattern          Send a trap when AntiVirus finds file matching pattern.
    av-fragmented      Send a trap when AntiVirus finds a fragmented file.
    fm-if-change        Send a trap when FortiManager interface changes. Send a FortiManager trap.
    fm-conf-change      Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
    bgp-established     Send a trap when a BGP FSM transitions to the established state.
    bgp-backward-transition Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.

```

```

    ha-member-up          Send a trap when an HA cluster member goes up.
    ha-member-down        Send a trap when an HA cluster member goes down.
    ent-conf-change        Send a trap when an entity MIB change occurs (RFC4133).
    av-conserve            Send a trap when the FortiGate enters conserve mode.
    av-bypass              Send a trap when the FortiGate enters bypass mode.
    av-oversize-passed     Send a trap when AntiVirus passes an oversized file.
    av-oversize-blocked   Send a trap when AntiVirus blocks an oversized file.
    ips-pkg-update         Send a trap when the IPS signature database or engine is updated.
    ips-fail-open          Send a trap when the IPS network buffer is full.
    temperature-high       Send a trap when a temperature sensor registers a temperature that is too high.
    voltage-alert          Send a trap when a voltage sensor registers a voltage that is outside of the normal range.
    power-supply-failure   Send a trap when a power supply fails.
    faz-disconnect         Send a trap when a FortiAnalyzer disconnects from the FortiGate.
    fan-failure            Send a trap when a fan fails.
    wc-ap-up               Send a trap when a managed FortiAP comes up.
    wc-ap-down             Send a trap when a managed FortiAP goes down.
    fswctl-session-up      Send a trap when a FortiSwitch controller session comes up.
    fswctl-session-down    Send a trap when a FortiSwitch controller session goes down.
    load-balance-real-server-down Send a trap when a server load balance real server goes down.
    device-new             Send a trap when a new device is found.
    per-cpu-high           Send a trap when per-CPU usage is high.
set security-level { no-auth-no-priv | auth-no-priv | auth-priv } Security level for message authentication and encryption.
    no-auth-no-priv Message with no authentication and no privacy (encryption).
    auth-no-priv Message with authentication but no privacy (encryption).
    auth-priv Message with authentication and privacy (encryption).
set auth-proto { md5 | sha } Authentication protocol.
    md5 HMAC-MD5-96 authentication protocol.
    sha HMAC-SHA-96 authentication protocol.
set auth-pwd { password_string } Password for authentication protocol. size[128]
set priv-proto { aes | des | aes256 | aes256cisco } Privacy (encryption) protocol.
    aes CFB128-AES-128 symmetric encryption protocol.
    des CBC-DES symmetric encryption protocol.
    aes256 CFB128-AES-256 symmetric encryption protocol.
    aes256cisco CFB128-AES-256 symmetric encryption protocol compatible with CISCO.
set priv-pwd { password_string } Password for privacy (encryption) protocol. size[128]
next
end

```

system storage

Introduction.

```
config system storage
  edit { name }
  # Configure logical storage.
  set name { string }  Storage name. size[35]
  set partition { string }  Label of underlying partition. size[16]
  set media-type { string }  Media of underlying disk. size[4]
  set device { string }  Partition device. size[12]
  set size { integer }  Partition size. range[0-4294967295]
  next
end
```

system stp

Introduction.

```
config system stp
  set switch-priority { option } 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).
    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
  set hello-time { integer } Hello time (1 - 10 sec, default = 2). range[1-10]
  set forward-delay { integer } Forward delay (4 - 30 sec, default = 15). range[4-30]
  set max-hops { integer } Maximum number of hops (1 - 40, default = 20). range[1-40]
  set region-name { string } Set region name. size[31]
  set config-revision { integer } STP configuration revision (0 - 4294967295, default = 0). range[0-4294967295]
  set max-age { integer } Maximum packet age (6 - 40 sec, default = 20). range[6-40]
end
```

system switch-interface

Introduction.

```
config system switch-interface
  edit { name }
  # Configure software switch interfaces by grouping physical and WiFi interfaces.
  set name { string }  Interface name (name cannot be in use by any other interfaces, VLANs, or inter-VDOM links). size[15]
  set vdom { string }  VDOM that the software switch belongs to. size[31] - datasource(s): system.vdom.name
  set span-dest-port { string }  SPAN destination port name. All traffic on the SPAN source ports is echoed to the SPAN destination port. size
[15] - datasource(s): system.interface.name
  config span-source-port
    edit { interface-name }
    # Physical interface name. Port spanning echoes all traffic on the SPAN source ports to the SPAN destination port.
    set interface-name { string }  Physical interface name. size[64] - datasource(s): system.interface.name
    next
  config member
    edit { interface-name }
    # Names of the interfaces that belong to the virtual switch.
    set interface-name { string }  Physical interface name. size[64] - datasource(s): system.interface.name
    next
  set type { switch | hub }  Type of switch based on functionality: switch for normal functionality, or hub to duplicate packets to all port
members.
    switch  Switch for normal switch functionality (available in NAT mode only).
    hub    Hub to duplicate packets to all member ports.
  set intra-switch-policy { implicit | explicit }  Allow any traffic between switch interfaces or require firewall policies to allow traffic
between switch interfaces.
    implicit  Traffic between switch members is implicitly allowed.
    explicit  Traffic between switch members must match firewall policies.
  set span { disable | enable }  Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span des-
tination port.
  set span-direction { rx | tx | both }  The direction in which the SPAN port operates, either: rx, tx, or both.
    rx    Copies only received packets from source SPAN ports to the destination SPAN port.
    tx    Copies only transmitted packets from source SPAN ports to the destination SPAN port.
    both  Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.
  next
end
```


system tos-based-priority

Introduction.

```
config system tos-based-priority
  edit { id }
    # Configure Type of Service (ToS) based priority table to set network traffic priorities.
    set id { integer } Item ID. range[0-4294967295]
    set tos { integer } 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). range[0-15]
    set priority { low | medium | high } ToS based priority level to low, medium or high (these priorities match firewall traffic shaping priorities) (default = medium).
      low Low priority.
      medium Medium priority.
      high High priority.
  next
end
```

system vdom

Introduction.

```
config system vdom
  edit { name }
  # Configure virtual domain.
  set name { string }   VDOM name. size[31]
  set short-name { string }   VDOM short name. size[11]
  set vcluster-id { integer }   Virtual cluster ID (0 - 4294967295). range[0-4294967295]
  set temporary { integer }   Temporary. range[0-4294967295]
next
end
```

system vdom-dns

Introduction.

```
config system vdom-dns
  set vdom-dns { enable | disable }  Enable/disable configuring DNS servers for the current VDOM.
  set primary { ipv4 address }  Primary DNS server IP address for the VDOM.
  set secondary { ipv4 address }  Secondary DNS server IP address for the VDOM.
  set ip6-primary { ipv6 address }  Primary IPv6 DNS server IP address for the VDOM.
  set ip6-secondary { ipv6 address }  Secondary IPv6 DNS server IP address for the VDOM.
  set source-ip { ipv4 address }  Source IP for communications with the DNS server.
end
```

system vdom-link

Introduction.

```
config system vdom-link
  edit { name }
  # Configure VDOM links.
  set name { string } VDOM link name (maximum = 8 characters). size[11]
  set vcluster { vcluster1 | vcluster2 } Virtual cluster.
    vcluster1 Virtual cluster 1.
    vcluster2 Virtual cluster 2.
  set type { ppp | ethernet } VDOM link type: PPP or Ethernet.
    ppp PPP VDOM link.
    ethernet Ethernet VDOM link.
  next
end
```

system vdom-netflow

Introduction.

```
config system vdom-netflow
  set vdom-netflow { enable | disable }  Enable/disable NetFlow per VDOM.
  set collector-ip { ipv4 address }  NetFlow collector IP address.
  set collector-port { integer }  NetFlow collector port number. range[0-65535]
  set source-ip { ipv4 address }  Source IP address for communication with the NetFlow agent.
end
```

system vdom-property

Introduction.

```
config system vdom-property
  edit { name }
  # Configure VDOM property.
  set name { string }   VDOM name. size[31] - datasource(s): system.vdom.name
  set description { string }   Description. size[127]
  set snmp-index { integer }   Permanent SNMP Index of the virtual domain (0 - 4294967295). range[0-4294967295]
  set session { string }   Maximum guaranteed number of sessions.
  set ipsec-phase1 { string }   Maximum guaranteed number of VPN IPsec phase 1 tunnels.
  set ipsec-phase2 { string }   Maximum guaranteed number of VPN IPsec phase 2 tunnels.
  set dialup-tunnel { string }   Maximum guaranteed number of dial-up tunnels.
  set firewall-policy { string }   Maximum guaranteed number of firewall policies.
  set firewall-address { string }   Maximum guaranteed number of firewall addresses.
  set firewall-addrgrp { string }   Maximum guaranteed number of firewall address groups.
  set custom-service { string }   Maximum guaranteed number of firewall custom services.
  set service-group { string }   Maximum guaranteed number of firewall service groups.
  set onetime-schedule { string }   Maximum guaranteed number of firewall one-time schedules.
  set recurring-schedule { string }   Maximum guaranteed number of firewall recurring schedules.
  set user { string }   Maximum guaranteed number of local users.
  set user-group { string }   Maximum guaranteed number of user groups.
  set sslvpn { string }   Maximum guaranteed number of SSL-VPNs.
  set proxy { string }   Maximum guaranteed number of concurrent proxy users.
  set log-disk-quota { string }   Log disk quota in MB (range depends on how much disk space is available).
  next
end
```

system vdom-radius-server

Introduction.

```
config system vdom-radius-server
  edit { name }
    # Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.
    set name { string } Name of the VDOM that you are adding the RADIUS server to. size[31] - datasource(s): system.vdom.name
    set status { enable | disable } Enable/disable the RSSO RADIUS server for this VDOM.
    set radius-server-vdom { string } Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.
size[31] - datasource(s): system.vdom.name
  next
end
```

system vdom-sflow

Introduction.

```
config system vdom-sflow
  set vdom-sflow { enable | disable }  Enable/disable the sFlow configuration for the current VDOM.
  set collector-ip { ipv4 address }  IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to
  (default = 0.0.0.0).
  set collector-port { integer }  UDP port number used for sending sFlow datagrams (configure only if required by your sFlow collector or your net-
  work configuration) (0 - 65535, default = 6343). range[0-65535]
  set source-ip { ipv4 address }  Source IP address for sFlow agent.
end
```


system virtual-switch

Introduction.

```
config system virtual-switch
  edit { name }
  # Configure virtual hardware switch interfaces.
  set span-direction { rx | tx | both } SPAN direction.
    rx Span receive direction only.
    tx Span transmit direction only.
    both Span both directions.
  set span-source-port { string } SPAN source ports. size[15]
  set span { disable | enable } Enable/disable SPAN.
  set physical-switch { string } Physical switch parent. size[15] - datasource(s): system.physical-switch.name
  set name { string } Name of the virtual switch. size[15]
  set span-dest-port { string } SPAN destination port. size[15]
  config port
    edit { name }
    # Configure member ports.
    set speed { option } Interface speed.
      auto Automatically adjust speed.
      10full 10M full-duplex.
      10half 10M half-duplex.
      100full 100M full-duplex.
      100half 100M half-duplex.
      1000full 1000M full-duplex.
      1000half 1000M half-duplex.
      1000auto 1000M auto adjust.
    set status { up | down } Interface status.
      up Interface up.
      down Interface down.
    set alias { string } Alias. size[25]
    set name { string } Physical interface name. size[15]
  next
end
```

system virtual-wan-link

Introduction.

```

config system virtual-wan-link
  set status { disable | enable }  Enable/disable SD-WAN.
  set load-balance-mode { option }  Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.
    source-ip-based      Source IP load balancing. All traffic from a source IP is routed out the same physical FortiGate interface.
    weight-based         Weight-based load balancing. More sessions are sent to interfaces with higher weights.
    usage-based          Usage-based or session-based load balancing. More new traffic is sent to interfaces that are processing fewer sessions.
    source-dest-ip-based Source and destination IP load balancing. All traffic from a source IP to a destination IP is routed out the same physical FortiGate interface.
    measured-volume-based Traffic volume-based load balancing. More traffic is sent to interfaces that have more available bandwidth.
  set fail-detect { enable | disable }  Enable/disable SD-WAN Internet connection status checking (failure detection).
  config fail-alert-interfaces
    edit { name }
      # Physical interfaces that will be alerted.
      set name { string }  Physical interface name. size[64] - datasource(s): system.interface.name
    next
  config members
    edit { seq-num }
      # Physical FortiGate interfaces added to the virtual-wan-link.
      set seq-num { integer }  Sequence number(1-255). range[0-255]
      set interface { string }  Interface name. size[15] - datasource(s): system.interface.name
      set gateway { ipv4 address }  The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
      set weight { integer }  Weight of this interface for weighted load balancing. (0 - 255) More traffic is directed to interfaces with higher weights. range[0-255]
      set priority { integer }  Priority of the interface (0 - 4294967295). Used for SD-WAN rules or priority rules. range[0-4294967295]
      set spillover-threshold { integer }  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. range[0-16776000]
      set ingress-spillover-threshold { integer }  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. range[0-16776000]
      set volume-ratio { integer }  Measured volume ratio (this value / sum of all values = percentage of link volume, 0 - 255). range[0-255]
      set status { disable | enable }  Enable/disable this interface in the SD-WAN.
    next
  config health-check
    edit { name }

```

```

# 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.
set name { string } Status check or health check name. size[35]
set server { string } IP address or FQDN name of the server. size[63]
set protocol { option } Protocol used to determine if the FortiGate can communicate with the server.
    ping Use PING to test the link with the server.
    tcp-echo Use TCP echo to test the link with the server.
    udp-echo Use UDP echo to test the link with the server.
    http Use HTTP-GET to test the link with the server.
    twamp Use TWAMP to test the link with the server.
set port { integer } Port number used to communicate with the server over the selected protocol. range[1-65535]
set security-mode { none | authentication } Twamp controller security mode.
    none Unauthenticated mode.
    authentication Authenticated mode.
set password { password_string } Twamp controller password in authentication mode size[128]
set packet-size { integer } Packet size of a twamp test session, range[64-1024]
set http-get { string } URL used to communicate with the server if the protocol is HTTP. size[1024]
set http-match { string } Response string expected from the server if the protocol is HTTP. size[1024]
set interval { integer } Status check interval, or the time between attempting to connect to the server (1 - 3600 sec, default = 5).
range[1-3600]
set timeout { integer } How long to wait before not receiving a reply from the server to consider the connection attempt a failure (1 - 255 sec, default = 1). range[1-255]
set failtime { integer } Number of failures before server is considered lost (1 - 10, default = 5). range[1-10]
set recoverytime { integer } Number of successful responses received before server is considered recovered (1 - 10, default = 5). range
[1-10]
set update-cascade-interface { enable | disable } Enable/disable update cascade interface.
set update-static-route { enable | disable } Enable/disable updating the static route.
set threshold-warning-packetloss { integer } Warning threshold for packet loss (percentage, default = 0). range[0-100]
set threshold-alert-packetloss { integer } Alert threshold for packet loss (percentage, default = 0). range[0-100]
set threshold-warning-latency { integer } Warning threshold for latency (ms, default = 0). range[0-4294967295]
set threshold-alert-latency { integer } Alert threshold for latency (ms, default = 0). range[0-4294967295]
set threshold-warning-jitter { integer } Warning threshold for jitter (ms, default = 0). range[0-4294967295]
set threshold-alert-jitter { integer } Alert threshold for jitter (ms, default = 0). range[0-4294967295]
next
config service
edit { id }
# Create SD-WAN rules or priority rules (also called services) to control how sessions are distributed to physical interfaces in the SD-WAN.
set id { integer } Priority rule ID (1 - 255). range[0-255]
set name { string } Priority rule name. size[35]
set mode { auto | manual | priority } Control how the priority rule sets the priority of interfaces in the SD-WAN.
    auto Assign interfaces a priority based on quality.
    manual Assign interfaces a priority manually.
    priority Assign interfaces a priority based on the priority assigned to the interface.

```

```
set quality-link { integer } Quality grade. range[0-255]
set member { integer } Member sequence number. range[0-255]
set tos { string } Type of service bit pattern.
set tos-mask { string } Type of service evaluated bits.
set protocol { integer } Protocol number. range[0-255]
set start-port { integer } Start destination port number. range[0-65535]
set end-port { integer } End destination port number. range[0-65535]
config dst
  edit { name }
  # Destination address name.
  set name { string } Address or address group name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
config src
  edit { name }
  # Source address name.
  set name { string } Address or address group name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
config users
  edit { name }
  # User name.
  set name { string } User name. size[64] - datasource(s): user.local.name
  next
config groups
  edit { name }
  # User groups.
  set name { string } Group name. size[64] - datasource(s): user.group.name
  next
set internet-service { enable | disable } Enable/disable use of Internet service for application-based load balancing.
config internet-service-custom
  edit { name }
  # Custom Internet service name list.
  set name { string } Custom Internet service name. size[64] - datasource(s): firewall.internet-service-custom.name
  next
config internet-service-id
  edit { id }
  # Internet service ID list.
  set id { integer } Internet service ID. range[0-4294967295] - datasource(s): firewall.internet-service.id
  next
set health-check { string } Health check. size[35]
set link-cost-factor { latency | jitter | packet-loss } Link cost factor.
  latency Select link based on latency.
  jitter Select link based on jitter.
  packet-loss Select link based on packet loss.
```

```
        set link-cost-threshold { integer } Percentage threshold change of link cost values that will result in policy route regeneration (0 -
10000000, default = 10).
    range[0-10000000]
    config priority-members
        edit { seq-num }
            # Member sequence number list.
            set seq-num { integer } Member sequence number. range[0-4294967295]
        next
    set status { disable | enable } Enable/disable virtual WAN link service.
next
end
```

system virtual-wire-pair

Introduction.

```
config system virtual-wire-pair
  edit { name }
  # Configure virtual wire pairs.
  set name { string }  Virtual-wire-pair name. Must be a unique interface name. size[35]
  config member
    edit { interface-name }
    # Interfaces belong to the virtual-wire-pair.
    set interface-name { string }  Interface name. size[64] - datasource(s): system.interface.name
    next
  set wildcard-vlan { enable | disable }  Enable/disable wildcard VLAN.
  next
end
```

system vxlan

Introduction.

```
config system vxlan
  edit { name }
  # Configure VXLAN devices.
  set name { string }  VXLAN device or interface name. Must be a unique interface name. size[15]
  set interface { string }  Outgoing interface for VXLAN encapsulated traffic. size[15] - datasource(s): system.interface.name
  set vni { integer }  VXLAN network ID. range[1-16777215]
  set ip-version { ipv4-unicast | ipv6-unicast | ipv4-multicast | ipv6-multicast }  IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast or multicast.
  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.
  config remote-ip
    edit { ip }
    # IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN.
    set ip { string }  IPv4 address. size[15]
    next
  config remote-ip6
    edit { ip6 }
    # IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN.
    set ip6 { string }  IPv6 address. size[45]
    next
  set dstport { integer }  VXLAN destination port (1 - 65535, default = 4789). range[1-65535]
  set multicast-ttl { integer }  VXLAN multicast TTL (1-255, default = 0). range[1-255]
  next
end
```

system wccp

Use this command to configure various settings for Web Cache Communication Protocol (WCCP). Before you can do this however, you must first configure the FortiGate as either a WCCP router or client: **FortiGate as WCCP router:** Intercepts HTTP and HTTPS sessions and forwards them to a web caching engine, caches web pages, and returns cached content to the web browser. **FortiGate as WCCP client:** Accepts and forwards WCCP sessions and uses firewall policies to apply NAT, UTM, and more security features. Note that FortiGates may only operate as clients while in NAT/Route mode (*not* in Transparent mode). To assign either role to the FortiGate, use the following command:

```
config system settings
    set wccp-cache-engine {enable | disable}
end
```

Set this command to `disable` (by default) for the FortiGate to operate as a WCCP **router**. Set this command to `enable` for the FortiGate to operate as a WCCP **client**. When enabled, an interface named `w.root` is added to the FortiGate (shown under `config system interfaces`). All WCCP sessions received by the FortiGate — operating as a WCCP client — are considered to be received at this interface, where you can enter firewall policies for WCCP traffic. **Note:** All WCCP entries created, whether for router or client, must be numbered within the range of 0-255. The default is set to 1. Use 0 for HTTP.

```
config system wccp
    edit { service-id }
        # Configure WCCP.
        set service-id { string }    Service ID. size[3]
        set router-id { ipv4 address }    IP address known to all cache engines. If all cache engines connect to the same FortiGate interface, use the
        default 0.0.0.0.
        set cache-id { ipv4 address }    IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.
        set group-address { multicast ipv4 address }    IP multicast address used by the cache routers. For the FortiGate to ignore multicast WCCP
        traffic, use the default 0.0.0.0.
        set server-list { string }    IP addresses and netmasks for up to four cache servers.
        set router-list { string }    IP addresses of one or more WCCP routers.
        set ports-defined { source | destination }    Match method.
            source    Source port match.
            destination    Destination port match.
        set ports { string }    Service ports.
        set authentication { enable | disable }    Enable/disable MD5 authentication.
        set password { password_string }    Password for MD5 authentication. size[128]
        set forward-method { GRE | L2 | any }    Method used to forward traffic to the cache servers.
            GRE    GRE encapsulation.
            L2    L2 rewrite.
```



```

        any GRE or L2.
set cache-engine-method { GRE | L2 } Method used to forward traffic to the routers or to return to the cache engine.
    GRE GRE encapsulation.
    L2 L2 rewrite.
set service-type { auto | standard | dynamic } WCCP service type used by the cache server for logical interception and redirection of
traffic.
    auto auto
    standard Standard service.
    dynamic Dynamic service.
set primary-hash { src-ip | dst-ip | src-port | dst-port } Hash method.
    src-ip Source IP hash.
    dst-ip Destination IP hash.
    src-port Source port hash.
    dst-port Destination port hash.
set priority { integer } Service priority. range[0-255]
set protocol { integer } Service protocol. range[0-255]
set assignment-weight { integer } Assignment of hash weight/ratio for the WCCP cache engine. range[0-255]
set assignment-bucket-format { wccp-v2 | cisco-implementation } Assignment bucket format for the WCCP cache engine.
    wccp-v2 WCCP-v2 bucket format.
    cisco-implementation Cisco bucket format.
set return-method { GRE | L2 | any } Method used to decline a redirected packet and return it to the FortiGate.
    GRE GRE encapsulation.
    L2 L2 rewrite.
    any GRE or L2.
set assignment-method { HASH | MASK | any } Hash key assignment preference.
    HASH HASH assignment method.
    MASK MASK assignment method.
    any HASH or MASK.
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

Router mode

The entries below are available when the FortiGate has been configured as a WCCP router.

router-id <ip-address>

IP address known to all cache engines, and identifies an interface on the FortiGate to the cache engines. If all cache engines connect to the same FortiGate interface, use the default address of 0.0.0.0. However, if the cache engines can connect to different FortiGate interfaces, you must set `router-id` to a specific IP address, which must then be added to the configuration of the cache engines that connect to that interface.

group-address <multicast-address>

IP multicast address used by the cache routers. The default, 0.0.0.0, means the FortiGate will ignore multicast WCCP traffic. Otherwise, set the address between 244.0.0.0 to 239.255.255.255.

server-list <router-1> [router-2] [router-3] [router-4]

IP address and netmask for up to four cache servers.

authentication {enable | disable}

Enable or disable (by default) use of MD5 authentication for the WCCP configuration.

password <password>

Note: This entry is only available when `authentication` is set to `enable`. Password for MD5 authentication (maximum length of eight characters).

forward-method {GRE | L2 | any}

Defines how the FortiGate forwards traffic to cache servers:

- **GRE:** Encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP server and a destination IP address of the target WCCP client. This allows the WCCP server to be multiple Layer 3 hops away from the WCCP client.
 - **L2:** Rewrites the destination MAC address of the intercepted packet to equal the MAC address of the target WCCP client. L2 forwarding requires that the WCCP server is Layer 2 adjacent to the WCCP client.
 - **any:** Cache server determines the method.
-

return-method {GRE | L2 | any}

Defines how a cache server declines a redirected packet, and returns it to the FortiGate (see `forward-method` above for option descriptions).

assignment-method {HASH | MASK | any}

Defines which assignment method the FortiGate prefers:

- **HASH:** A hash key based on any combination of the source and destination IP and port of the packet.
 - **MASK:** A mask value specified with a maximum of 7 bits and, like the hash key, can be configured to cover both the source and destination address space.
 - **any:** Cache server determines the method.
-

Client mode

The entries below are available when the FortiGate has been configured as a WCCP client.

cache-id <ip-address>

IP address of the cache engine if its IP address is not the same as the IP address of a FortiGate interface. If the addresses are the same, use the default address of `0.0.0.0`.

group-address <multicast-address>

IP multicast address used by the cache routers. The default, `0.0.0.0`, means the FortiGate will ignore multicast WCCP traffic. Otherwise, set the address between `244.0.0.0` to `239.255.255.255`.

router-list <addresses>

IP addresses of one or more WCCP routers that can communicate with a FortiGate operating as a WCCP cache engine. Separate multiple addresses with spaces.

authentication {enable | disable}

Enable or disable (by default) use of MD5 authentication for the WCCP configuration.

cache-engine-method {GRE | L2}

Defines how traffic is forwarded to routers or returned to the cache engine (see `forward-method` above for option descriptions). The default is set to `GRE`.

service-type {auto | standard | dynamic}

WCCP service type, or service group, used by the cache server for logical interception and redirection of traffic. The default is set to `auto`.

- **auto:** Transparent redirection of traffic, whereby the target URL is used to request content, and have requests automatically redirected to a web caching engine.
 - **standard:** Intercepts TCP port 80 (HTTP) traffic to the client.
 - **dynamic:** Use for when the router is instructed which protocol or ports to intercept, and how to distribute the traffic.
-

assignment-weight <weight>

Assignment weight/ratio for the WCCP cache engine. Set the value between 0-255. The default is set to 0.

assignment-bucket-format {wccp-v2 | cisco-implementation}

Assignment bucket format for the WCCP cache engine. WCCP version 2 (`wccp-v2`) allows for support of up to 256 masks. The default is set to `cisco-implementation`.

system wireless ap-status

Use this command to configure accepted wireless APs and their status.

```
config system wireless ap-status
  edit { id }
    # Configure accepted wireless AP.
```

```
set id { integer } AP ID. range[0-4294967295]
set bssid { mac address } AP's BSSID.
set ssid { string } AP's ssid size[32]
set status { rogue | accepted | suppressed } AP status.
    rogue Rogue.
    accepted Accepted.
    suppressed Suppressed.
next
end
```

system wireless settings

Use this command to configure wireless settings.

```
config system wireless settings
  set mode { CLIENT | AP | SCAN } Mode.
    CLIENT Client.
    AP Access point.
    SCAN Scan.
  set band { option } Band.
    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.
  set geography { option } Geography.
    World World.
    Americas Americas.
    EMEA EMEA.
    Israel Israel.
    Japan Japan.
  set channel { integer } Channel. range[0-4294967295]
  set power-level { integer } Power level (0 - 17). range[0-17]
  set beacon-interval { integer } Beacon level (25 - 1000). range[25-1000]
```

```
set short-guard-interval { enable | disable }  Enable/disable short guard interval.
set channel-bonding { enable | disable }  Supported channel width.
set bgscan { disable | enable }  Enable/disable background rogue AP scan.
set bgscan-interval { integer }  Interval between two rounds of scanning (15 - 3600 sec). range[15-3600]
set bgscan-idle { integer }  Interval between scanning channels (100 - 1000 ms). range[100-1000]
set rogue-scan { enable | disable }  Enable/disable rogue scan.
set rogue-scan-mac-adjacency { integer }  MAC adjacency (0-31). range[0-31]
end
```

system zone

Introduction.

```
config system zone
  edit { name }
  # Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual inter-
  faces in the zone.
  set name { string } Zone name. size[35]
  set intrazone { allow | deny } Allow or deny traffic routing between different interfaces in the same zone (default = deny).
    allow Allow traffic between interfaces in the zone.
    deny Deny traffic between interfaces in the zone.
  config interface
    edit { interface-name }
    # Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined.
    set interface-name { string } Select two or more interfaces to add to the zone. size[64] - datasource(s): system.interface.name
  next
next
end
```

user

Use `config user` to configure:

- external authentication servers
- user accounts and user groups for firewall policy authentication, SSL VPN authentication, administrator authentication and some types of VPN authentication
- device detection
- peers/peer groups for IPSec VPN and PKI user authentication.

This section includes syntax for the following commands:

- `user adgrp`
- `user device`
- `user device-access-list`
- `user device-category`
- `user device-group`
- `user fortitoken`
- `user fsso`
- `user fsso-polling`
- `user group`
- `user krb-keytab`
- `user ldap`
- `user local`
- `user password-policy`
- `user peer`
- `user peergrp`
- `user pop3`
- `user radius`
- `user security-exempt-list`
- `user setting`
- `user tacacs+`

user adgrp

Configure or edit existing Fortinet Single Sign-On (FSSO) groups. The command below creates a group that defines FSSO agent names and their polling ID.

```
config user adgrp
  edit { name }
  # Configure FSSO groups.
  set name { string } Name. size[511]
  set server-name { string } FSSO agent name. size[35] - datasource(s): user.fsso.name
  next
end
```

server-name <name>

FSSO agent name.

polling-id <id>

FSSO polling ID. Set value between 0-4294967295. The default is set to 0.

user device

Use this command to define and configure host devices.

```
config user device
  edit { alias }
  # Configure devices.
  set alias { string } Device alias. size[35]
  set mac { mac address } Device MAC address(es).
  set user { string } User name. size[64]
  set master-device { string } Master device (optional). size[35] - datasource(s): user.device.alias
  set comment { string } Comment. size[255]
  set avatar { string } Image file for avatar (maximum 4K base64 encoded). size[4095]
  config tags
    edit { name }
    # Applied object tags.
    set name { string } Tag name. size[64] - datasource(s): system.object-tag.name
  next
  set type { option } Device type.
    android-phone Android-based phones.
    android-tablet Android-based tablets.
    blackberry-phone BlackBerry phones.
    blackberry-playbook BlackBerry tablets.
    forticam FortiCam.
    fortifone FortiFone.
    fortinet-device Other Fortinet devices.
    gaming-console Gaming consoles (Xbox, PS2, PS3, Wii, PSP).
    ip-phone VoIP phones.
    ipad iPad Tablets.
    iphone iPhone and iPod Touch devices.
    linux-pc Linux PC.
    mac Mac computers.
    media-streaming Other media streaming devices.
    printer Printing devices.
    router-nat-device Router and/or NAT devices.
    windows-pc Windows PC.
    windows-phone Windows-based phones.
    windows-tablet Windows-based tablets.
    other-network-device All other identified devices.
```

```
    next
end
```

append tags <tag-name>

Append applied object tags.

mac <mac-address>

Enter the device's MAC address.

user <name>

Enter the device owner's user name.

master-device [name]

Optionally enter a master device name.

comment [string]

Optional comments.

avatar <image-file>

Enter an image file name to be used as the user's avatar (maximum 4K base64 encoded).

tags <image-file>

Enter applied object tags.

type <device-type>

Select the device type from the following:

- android-phone
- android-tablet
- blackberry-phone
- blackberry-playbook
- forticam
- fortifone
- fortinet-device
- gaming-console
- ip-phone
- ipad
- iphone
- linux-pc
- mac
- media-streaming
- printer
- router-nat-device
- windows-pc
- windows-phone
- windows-tablet
- other-network-device

user device-access-list

Use this command to configure device lists for use on interfaces with device identification enabled.

```
config user device-access-list
  edit { name }
  # Configure device access control lists.
  set name { string } Device access list name. size[35]
  set default-action { accept | deny } Accept or deny unknown/unspecified devices.
    accept Accept.
    deny Deny.
  config device-list
    edit { id }
    # Device list.
    set id { integer } Entry ID. range[0-4294967295]
    set device { string } Firewall device or device group. size[35] - datasource(s): user.device.alias,user.device-group.-
name,user.device-category.name
    set action { accept | deny } Allow or block device.
      accept Accept.
      deny Deny.
    next
  next
end
```

config device-list

A configuration method to create device name entries and define their action.

device <device-group>

Enter the firewall device or device group.

action {accept | deny}

Accept (by default) or deny the device.

default-action {accept | deny}

Select whether to accept (by default) or deny unknown/unspecified devices.

user device-category

Use this command to view all available device types/categories.

```
config user device-category
  edit { name }
  # Configure device categories.
  set name { string } Device category name. size[35]
  set desc { string } Device category description. size[255]
  set comment { string } Comment. size[255]
next
end
```

user device-group

Use this command to edit or define FortiGate default or custom device groups.

```
config user device-group
  edit { name }
  # Configure device groups.
  set name { string } Device group name. size[35]
  config member
    edit { name }
    # Device group member.
    set name { string } Device name. size[35] - datasource(s): user.device.alias,user.device-category.name
    next
  set comment { string } Comment. size[255]
next
end
```

append member <device>

Append device names/categories.

member <group-member>

Enter the device group members that belong to this group, each separated by a space (see the full default [list of device categories](#)).

comment [string]

Optional comments.

user fortitoken

Use this command to register and view FortiTokens.

```
config user fortitoken
  edit { serial-number }
  # Configure FortiToken.
  set serial-number { string }  Serial number. size[16]
  set status { active | lock }  Status
    active  Activate FortiToken.
    lock    Lock FortiToken.
  set seed { string }  Token seed. size[200]
  set comments { string }  Comment. size[255]
  set license { string }  Mobile token license. size[31]
  set activation-code { string }  Mobile token user activation-code. size[32]
  set activation-expire { integer }  Mobile token user activation-code expire time. range[0-4294967295]
  set reg-id { string }  Device Reg ID. size[256]
  set os-ver { string }  Device Mobile Version. size[15]
  next
end
```

status {active | lock}

Activate (by default) or lock the FortiToken.

comments [string]

Optional comments.

license <license>

Enter the FortiToken Mobile license. You can retrieve the token's license by entering `get`, or by using its activation-code in the following command:

```
execute fortitoken-mobile import <activation-code>
```

activation-code <code>

Note: This entry is *not* configurable from the CLI. From the GUI, the token must be assigned to a user and the activation code sent from the FortiGate to the user's email.

activation-expire <expire-time>

Note: This entry is *not* configurable from the CLI. From the GUI, the token must be assigned to a user and the activation code sent from the FortiGate to the user's email. The email will tell the user by when they must activate their token.

user fssso

Use this command to configure the FortiGate unit to receive user group information from a Directory Service server equipped with the Fortinet Single Sign-On (FSSO) Agent. You can specify up to five computers on which an FSSO collector agent is installed. The FortiGate unit uses these collector agents in a redundant configuration, whereby if the first agent fails, the FortiGate unit attempts to connect to the next agent in the list, and so on.

```
config user fssso
  edit { name }
    # Configure Fortinet Single Sign On (FSSO) agents.
    set name { string } Name. size[35]
    set server { string } Domain name or IP address of the first FSSO collector agent. size[63]
    set port { integer } Port of the first FSSO collector agent. range[1-65535]
    set password { password_string } Password of the first FSSO collector agent. size[128]
    set server2 { string } Domain name or IP address of the second FSSO collector agent. size[63]
    set port2 { integer } Port of the second FSSO collector agent. range[1-65535]
    set password2 { password_string } Password of the second FSSO collector agent. size[128]
    set server3 { string } Domain name or IP address of the third FSSO collector agent. size[63]
    set port3 { integer } Port of the third FSSO collector agent. range[1-65535]
    set password3 { password_string } Password of the third FSSO collector agent. size[128]
    set server4 { string } Domain name or IP address of the fourth FSSO collector agent. size[63]
    set port4 { integer } Port of the fourth FSSO collector agent. range[1-65535]
    set password4 { password_string } Password of the fourth FSSO collector agent. size[128]
    set server5 { string } Domain name or IP address of the fifth FSSO collector agent. size[63]
    set port5 { integer } Port of the fifth FSSO collector agent. range[1-65535]
    set password5 { password_string } Password of the fifth FSSO collector agent. size[128]
    set ldap-server { string } LDAP server to get group information. size[35] - datasource(s): user.ldap.name
    set source-ip { ipv4 address } Source IP for communications to FSSO agent.
  next
end
```

{server | server2 | server3 | server4 | server5} <agent-address>

Enter the domain name or IP address for up to five collector agents (maximum of 63 characters).

{port | port2 | port3 | port4 | port5} <agent-port>

For each collector agent, enter the port number used for communication with FortiGate units. The default, for each port, is set to 8000.

{password | password2 | password3 | password4 | password5} <agent-password>

For each collector agent, enter the password.

ldap-server <server>

Enter the name of the LDAP server to be used to get group information from the Directory Service.

source-ip <server>

Enter the source IP for communications to FSSO servers.

user fsso-polling

Use this command to configure polling of servers for FSSO. Edit to define separate ID numbers for the Windows AD server.

```
config user fsso-polling
  edit { id }
    # Configure FSSO active directory servers for polling mode.
    set id { integer } Active Directory server ID. range[0-4294967295]
    set status { enable | disable } Enable/disable polling for the status of this Active Directory server.
    set server { string } Host name or IP address of the Active Directory server. size[63]
    set default-domain { string } Default domain managed by this Active Directory server. size[35]
    set port { integer } Port to communicate with this Active Directory server. range[0-65535]
    set user { string } User name required to log into this Active Directory server. size[35]
    set password { password_string } Password required to log into this Active Directory server size[128]
    set ldap-server { string } LDAP server name used in LDAP connection strings. size[35] - datasource(s): user.ldap.name
    set logon-history { integer } Number of hours of logon history to keep, 0 means keep all history. range[0-48]
    set polling-frequency { integer } Polling frequency (every 1 to 30 seconds). range[1-30]
  config adgrp
    edit { name }
      # LDAP Group Info.
      set name { string } Name. size[511]
    next
  next
end
```

config adgrp

Note: This entry is *not* configurable.

status {enable | disable}

Enable (by default) or disable FSSO polling.

server <name/ip>

Name or IP address of the AD server.

default-domain <domain>

This server's default domain name.

port {port}

Server port number. Set the value between 0-65535. The default is set to 0.

user <user>

User name for the AD server.

password <password>

AD server password.

ldap-server <server>

Name of the LDAP server for group and user names.

logon-history <hours>

Amount of time in hours to maintain active logon. Set the value between 1-48 (or one hour to two days). The default is set to 8. Set to 0 to for no time limit.

polling-frequency <frequency>

Interval time in seconds that polling occurs. Set the value between 1-30. The default is set to 10.

user group

Use this command to add or edit user groups. User groups can include defined peer users.

```

config user group
  edit { name }
  # Configure user groups.
  set name { string }   Group name. size[35]
  set id { integer }   Group ID. range[0-4294967295]
  set group-type { firewall | fssso-service | rssp | guest }   Set the group to be for firewall authentication, FSSO, RSSO, or guest users.
    firewall           Firewall.
    fssso-service      Fortinet Single Sign-On Service.
    rssp               RADIUS based Single Sign-On Service.
    guest              Guest.
  set authtimeout { integer }   Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout. range[0-43200]
  set auth-concurrent-override { enable | disable }   Enable/disable overriding the global number of concurrent authentication sessions for this user group.
  set auth-concurrent-value { integer }   Maximum number of concurrent authenticated connections per user (0 - 100). range[0-100]
  set http-digest-realm { string }   Realm attribute for MD5-digest authentication. size[35]
  set sso-attribute-value { string }   Name of the RADIUS user group that this local user group represents. size[511]
  config member
    edit { name }
    # Names of users, peers, LDAP servers, or RADIUS servers to add to the user group.
    set name { string }   Group member name. size[511] - datasource(s): user-peer.name,user.local.name,user.radius.name,user.tacacs+.name,user.ldap.name,user.adgrp.name,user.pop3.name
    next
  config match
    edit { id }
    # Group matches.
    set id { integer }   ID. range[0-4294967295]
    set server-name { string }   Name of remote auth server. size[35] - datasource(s): user.radius.name,user.ldap.name,user.tacacs+.name
    set group-name { string }   Name of matching group on remote authentication server. size[511]
    next
  set user-id { email | auto-generate | specify }   Guest user ID type.
    email           Email address.
    auto-generate   Automatically generate.
    specify         Specify.
  set password { auto-generate | specify | disable }   Guest user password type.

```

```

        auto-generate Automatically generate.
        specify Specify.
        disable Disable.
set user-name { disable | enable } Enable/disable the guest user name entry.
set sponsor { optional | mandatory | disabled } Set the action for the sponsor guest user field.
    optional Optional.
    mandatory Mandatory.
    disabled Disabled.
set company { optional | mandatory | disabled } Set the action for the company guest user field.
    optional Optional.
    mandatory Mandatory.
    disabled Disabled.
set email { disable | enable } Enable/disable the guest user email address field.
set mobile-phone { disable | enable } Enable/disable the guest user mobile phone number field.
set sms-server { fortiguard | custom } Send SMS through FortiGuard or other external server.
    fortiguard Send SMS by FortiGuard.
    custom Send SMS by custom server.
set sms-custom-server { string } SMS server. size[35] - datasource(s): system.sms-server.name
set expire-type { immediately | first-successful-login } Determine when the expiration countdown begins.
    immediately Immediately.
    first-successful-login First successful login.
set expire { integer } Time in seconds before guest user accounts expire. (1 - 31536000 sec) range[1-31536000]
set max-accounts { integer } Maximum number of guest accounts that can be created for this group (0 means unlimited). range[0-1024]
set multiple-guest-add { disable | enable } Enable/disable addition of multiple guests.
config guest
    edit { user-id }
        # Guest User.
        set user-id { string } Guest ID. size[64]
        set name { string } Guest name. size[64]
        set password { password_string } Guest password. size[128]
        set mobile-phone { string } Mobile phone. size[35]
        set sponsor { string } Set the action for the sponsor guest user field. size[35]
        set company { string } Set the action for the company guest user field. size[35]
        set email { string } Email. size[64]
        set expiration { string } Expire time.
        set comment { string } Comment. size[255]
    next
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

config guest

Note: When `group-type` is set to `guest`, `guest` options will become available and can be set. This configuration method will also become available, however it is *not* configurable.

config match

Note: This entry is only available when `group-type` is set to `firewall`. A configuration method to specify the user group names on the authentication servers that are members of this FortiGate user group. Note that if no matches are specified then all users on the server can authenticate.

server-name <name>

The name of the remote authentication server.

group-name <name>

The name of the matching group on the remote authentication server.

group-type {firewall | fsservice | rso | guest}

Type of group, which determines the type of user.

- `firewall`: Those users defined in the `user local`, `user ldap`, or `user radius` commands
- `fsservice`: Fortinet Single Sign-On (FSSO) users
- `rso`: RADIUS Single Sign-On (RSSO) users
- `guest`: Guest users

authtimeout <timeout>

Period of time in minutes before the authentication timeout for a user group is reached. Set the value between 1-4320 (or one minute to three days). The default is set to 0, which sets the timeout to use the global authentication value.

sso-attribute-value <attribute>

Note: This entry is only available when `group-type` is set to `rsso`. The name of the RADIUS user group that this local user group represents.

auth-concurrent-override {enable | disable}

Note: This entry is only available when `group-type` is set to either `firewall` OR `guest`. Enable or disable (by default) overriding the `policy-auth-concurrent` entry in the `system global` command.

auth-concurrent-value <limit>

Note: This entry is only available when `auth-concurrent-override` is set to `enable`. The number of concurrent logins permitted from the same user. Set the value between 1-100, or 0 (by default) for unlimited.

http-digest-realm <attribute>

Note: This entry is *not* available when `group-type` is set to `rsso`. The realm attribute for MD5-digest authentication.

user-id {email | auto-generate | specify}

Note: This entry is only available when `group-type` is set to `guest`. The source of the guest user ID.

- `email`: Use the guest's email address (by default).
 - `auto-generate`: Create a random user ID.
 - `specify`: Enter a user ID string.
-

password {auto-generate | specify | disable}

Note: This entry is only available when `group-type` is set to `guest`. The source of the guest password.

- `auto-generate`: Create a random user password (by default).
 - `specify`: Enter a user password string.
 - `disable`: Disables guest user's need for a password.
-

user-name {enable | disable}

Note: This entry is only available when `group-type` is set to `guest`. Enable or disable (by default) the guest user name entry.

sponsor {optional | mandatory | disable}

Note: This entry is only available when `group-type` is set to `guest`. Determines whether the sponsor field on the web-based manager Guest Management form should be optional (by default), mandatory, or disabled.

company {optional | mandatory | disable}

Note: This entry is only available when `group-type` is set to `guest`. Determines whether the guest's company name field on the web-based manager Guest Management form should be optional (by default), mandatory, or disabled.

email {enable | disable}

Note: This entry is only available when `group-type` is set to `guest`. Enable (by default) or disable the email address field in the web-based manager Guest Management form.

mobile-phone {enable | disable}

Note: This entry is only available when `group-type` is set to `guest`. Enable or disable (by default) the mobile phone number field in the web-based manager Guest Management form.

expire-type {immediately | first-successful-login}

Note: This entry is only available when `group-type` is set to `guest`. Determines when the expiry time countdown begins: immediately (by default) or after the user's first successful login.

expire <seconds>

Note: This entry is only available when `group-type` is set to `guest`. The time in seconds the user account has until it expires. Set the value between 1-31536000 (or one second to 365 days). The default is set to 14400.

max-accounts <limit>

Note: This entry is only available when `group-type` is set to `guest`. The maximum number of accounts permitted. The maximum value that can be set depends on the platform. The default is set to 0, or unlimited.

multiple-guest-add {enable | disable}

Note: This entry is only available when `group-type` is set to `guest`. Enable or disable (by default) the multiple guest add option in the web-based manager User Group form.

member <member>

Note: This entry is only available when `group-type` is set to either `firewall` or `fsso-service`. The names of users, peers, LDAP servers, or RADIUS servers to add to the user group, each separated by a space. Note that, to add or remove names from the group, you must re-enter the whole list with the required additions or deletions. . The names of users, peers, LDAP servers, or RADIUS servers to add to the user group, each separated by a space. Note that, to add or remove names from the group, you must re-enter the whole list with the required additions or deletions.

user krb-keytab

Use this command to configure Kerberos keytab entries. Keytab files are used to authenticate to various remote systems using Kerberos without entering a password, and without requiring human interaction or access to password stored in a plain-text file. The script is then able to use the acquired credentials to access files stored on a remote system.

```
config user krb-keytab
  edit { name }
    # Configure Kerberos keytab entries.
    set name { string }   Kerberos keytab entry name. size[35]
    set principal { string } Kerberos service principal, e.g. HTTP/fgt.example.com@EXAMPLE.COM. size[511]
    set ldap-server { string } LDAP server name. size[35] - datasource(s): user.ldap.name
    set keytab { string }   base64 coded keytab file containing a pre-shared key. size[2047]
  next
end
```

principal <principal>

The Kerberos service principal, e.g. HTTP/fgt.example.com@EXAMPLE.COM.

ldap-server <server>

The LDAP server name.

keytab <keytab>

The base64 coded keytab file containing a pre-shared key.

user ldap

Use this command to add or edit the definition of an LDAP server for user authentication. The maximum number of remote LDAP servers that can be configured for authentication is 10. LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication. With PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

```
config user ldap
edit { name }
# Configure LDAP server entries.
set name { string } LDAP server entry name. size[35]
set server { string } LDAP server CN domain name or IP. size[63]
set secondary-server { string } Secondary LDAP server CN domain name or IP. size[63]
set tertiary-server { string } Tertiary LDAP server CN domain name or IP. size[63]
set source-ip { ipv4 address } Source IP for communications to LDAP server.
set cnid { string } Common name identifier for the LDAP server. The common name identifier for most LDAP servers is "cn". size[20]
set dn { string } Distinguished name used to look up entries on the LDAP server. size[511]
set type { simple | anonymous | regular } Authentication type for LDAP searches.
    simple Simple password authentication without search.
    anonymous Bind using anonymous user search.
    regular Bind using username/password and then search.
set username { string } Username (full DN) for initial binding. size[511]
set password { password_string } Password for initial binding. size[128]
set group-member-check { user-attr | group-object | posix-group-object } Group member checking methods.
    user-attr User attribute checking.
    group-object Group object checking.
    posix-group-object POSIX group object checking.
set group-search-base { string } Search base used for group searching. size[511]
set group-object-filter { string } Filter used for group searching. size[2047]
set group-filter { string } Filter used for group matching. size[2047]
set secure { disable | starttls | ldaps } Port to be used for authentication.
    disable No SSL.
    starttls Use StartTLS.
    ldaps Use LDAPS.
set ca-cert { string } CA certificate name. size[63] - datasource(s): vpn.certificate.ca.name
set port { integer } Port to be used for communication with the LDAP server (default = 389). range[1-65535]
set password-expiry-warning { enable | disable } Enable/disable password expiry warnings.
set password-renewal { enable | disable } Enable/disable online password renewal.
set member-attr { string } Name of attribute from which to get group membership. size[63]
```

```
    set account-key-processing { same | strip }  Account key processing operation, either keep or strip domain string of UPN in the token.
        same  Same as UPN.
        strip Strip domain string from UPN.
    set account-key-name { string }  Account key name, using the UPN as the search filter. size[20]
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

append search-type

Append nested-user-group chain information.

server <name/ip>

LDAP server CN domain name or IP address. The host name must comply with [RFC1035](#).

secondary-server [name/ip]

Optionally, enter a second LDAP server name or IP.

tertiary-server [name/ip]

Optionally, enter a third LDAP server name or IP.

source-ip [class-ip]

Optionally, enter a source IP address to be used for LDAP requests.

cnid <id>

Common name identifier for the LDAP server (maximum of 20 characters). The default is set to `cn`, which is the common name identifier for most LDAP servers. However some servers use other common name identifiers such as `uid`.

dn <dn>

Note: You must provide a `dn` value if `type` is set to `simple`. Distinguished name used to look up entries on the LDAP server (maximum of 512 characters). The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. The FortiGate unit passes this distinguished name unchanged to the server.

type {simple | anonymous | regular}

Note: You must provide a `dn` value if `type` is set to `simple`. Authentication type for LDAP searches.

- `simple`: Simple password authentication without search. Use if the user records are all under one distinguished name that you know. Otherwise, using either `anonymous` or `regular` will search the entire LDAP database for the required user name.
 - `anonymous`: Bind using anonymous user search.
 - `regular`: Bind using username/password and then search. Use if your LDAP server requires authentication to perform searches, providing values for username and password.
-

group-member-check {user-attr | group-object | posix-group-object}

Group member checking methods.

- `user-attr`: Check user attributes (by default).
 - `group-object`: Check group objects.
 - `posix-group-object`: Checks Portable Operating System Interface (POSIX) group objects.
-

secure {disable | starttls | ldaps}

Port to be used in authentication.

- `disable`: Port 389 (by default)
- `starttls`: Port 389
- `ldaps`: Port 636

port <port>

Port number to be used for communication with the LDAP server. Set the value between 1-65535. The default is set to 389.

password-expiry-warning {enable | disable}

Enable or disable (by default) password expiry warnings.

password-renewal {enable | disable}

Enable or disable (by default) online password renewal.

member-attr <attribute-name>

Name of attribute from which to get group membership. The default is set to `memberOf`. Examples are shown below: . Examples are shown below:

- `memberOf` for Windows AD and OpenLDAP
- `groupMembership` for eDirectory

search-type {nested}

Retrieve the complete nested-user-group chain information of a user in a particular Microsoft AD domain.

account-key-processing {same | strip}

Account key processing operation, an option to keep or strip domain string of User Principal Name (UPN) in the token.

- `same`: Same as UPN. This is set by default.
- `strip`: Strip domain string from UPN.

UPN is a logon method of authentication where you enter the credentials as `username@domainname.com` instead of the Windows authentication method, `domainname\username`.

account-key-name <name>

Account key name, using the UPN as the search filter.

user local

Use this command to add or edit local users and their authentication options, such as two-factor authentication.

Note: To add authentication by RADIUS, TACACS+, or LDAP server, you *must* first add servers using the [user radius](#), [user tacacs+](#), or [user ldap](#) commands respectively.

```
config user local
edit { name }
# Configure local users.
set name { string } User name. size[64]
set id { integer } User ID. range[0-4294967295]
set status { enable | disable } Enable/disable allowing the local user to authenticate with the FortiGate unit.
set type { password | radius | tacacs+ | ldap } Authentication method.
    password Password authentication.
    radius RADIUS server authentication.
    tacacs+ TACACS+ server authentication.
    ldap LDAP server authentication.
set passwd { password_string } User's password. size[128]
set ldap-server { string } Name of LDAP server with which the user must authenticate. size[35] - datasource(s): user.ldap.name
set radius-server { string } Name of RADIUS server with which the user must authenticate. size[35] - datasource(s): user.radius.name
set tacacs+-server { string } Name of TACACS+ server with which the user must authenticate. size[35] - datasource(s): user.tacacs+.name
set two-factor { disable | fortitoken | email | sms } Enable/disable two-factor authentication.
    disable disable
    fortitoken FortiToken
    email Email authentication code.
    sms SMS authentication code.
set fortitoken { string } Two-factor recipient's FortiToken serial number. size[16] - datasource(s): user.fortitoken.serial-number
set email-to { string } Two-factor recipient's email address. size[63]
set sms-server { fortiguard | custom } Send SMS through FortiGuard or other external server.
    fortiguard Send SMS by FortiGuard.
    custom Send SMS by custom server.
set sms-custom-server { string } Two-factor recipient's SMS server. size[35] - datasource(s): system.sms-server.name
set sms-phone { string } Two-factor recipient's mobile phone number. size[15]
set passwd-policy { string } Password policy to apply to this user, as defined in config user password-policy. size[35] - datasource(s):
user.password-policy.name
set passwd-time { string } Time of the last password update.
set authtimeout { integer } Time in minutes before the authentication timeout for a user is reached. range[0-1440]
set workstation { string } Name of the remote user workstation, if you want to limit the user to authenticate only from a particular
```

```
workstation. size[35]
    set auth-concurrent-override { enable | disable } Enable/disable overriding the policy-auth-concurrent under config system global.
    set auth-concurrent-value { integer } Maximum number of concurrent logins permitted from the same user. range[0-100]
next
end
```

status {enable | disable}

Enable (by default) or disable allowing the local user to authenticate with the FortiGate unit.

type {password | radius | tacacs+ | ldap}

Method in which the user's password is verified.

- `password`: Once set, enter a password in the `passwd` entry (see entry below). The FortiGate unit will verify the password against this value.
- `radius`: Once set, enter the server name in the `radius-server` entry (see entry below). The specified RADIUS server will verify the password.
- `tacacs+`: Once set, enter the server name in the `tacacs+-server` entry (see entry below). The specified TACACS+ server will verify the password.
- `ldap`: Once set, enter the server name in the `ldap-server` entry (see entry below). The specified LDAP server will verify the password.

passwd <password>

Note: This entry is only available when `type` is set to `password`. The user's password used to authenticate themselves. It is recommended to enter an alphanumeric password of at least six characters in length.

radius-server <server>

Note: This entry is only available when `type` is set to `radius`. Enter the name of the RADIUS server with which the user must authenticate.

tacacs+-server <server>

Note: This entry is only available when `type` is set to `tacacs+`. Enter the name of the TACACS+ server with which the user must authenticate.

ldap-server <server>

Note: This entry is only available when `type` is set to `ldap`. Enter the name of the LDAP server with which the user must authenticate. Enter the name of the LDAP server with which the user must authenticate.

two-factor {disable | fortitoken | email | sms}

Apply two-factor authentication through either FortiToken, email, or SMS, or disable it (by default). If set to `fortitoken`, use the `fortitoken` entry to assign a FortiToken to the user (see entry below).

fortitoken <token>

Note: This entry is only available when `two-factor` is set to `fortitoken`. Two-factor recipient's FortiToken serial number. The FortiToken must have already been added to the FortiGate unit to be set here.

email-to <address>

Two-factor recipient's email address.

sms-server {fortiguard | custom}

Send SMS through FortiGuard or other external server.

- `fortiguard`: Send SMS by FortiGuard (by default).
 - `custom`: Send SMS by custom server. Once set, use the `sms-custom-server` entry below to set the external server (see entry below).
-

sms-custom-server <server>

Note: This entry is only available when `sms-server` is set to `custom`. Name of the custom server to use for SMS-based two-factor authentication. Note that the server must have already been defined using the `system sms-server` command.

sms-phone <number>

User's phone number to be used for SMS-based two-factor authentication.

passwd-policy [policy]

Note: This entry is only available when `type` is set to `password`. Optionally, select a password policy to apply to this user. Use the `user password-policy` command to create password policies.

passwd-time

Note: This entry is only available when `type` is set to `password`. Displays the time of the last password update in the following format: `<yyyy-mm-dd hh:mm:ss>`.

authtimeout <timeout>

Period of time in minutes before the authentication timeout for a user is reached. Set the value between 1-1440 (or one minute to one day). The default is set to 0, which sets the timeout to use the global authentication value.

workstation <name>

Note: This entry is only available when `type` is set to `ldap`. Name of the remote user workstation. Set this value if you want to permit the user to authenticate *only* from a particular workstation.

auth-concurrent-override {enable | disable}

Enable or disable (by default) overriding the `policy-auth-concurrent` entry in the `system global` command.

auth-concurrent-value <limit>

Note: This entry is only available when `auth-concurrent-override` is set to `enable`. The number of concurrent logins permitted from the same user. Set the value between 1-100, or 0 (by default) for unlimited.

user password-policy

Use this command to create password policies that warn users that their password will expire. When a configurable number of days has been reached, the user will have the opportunity to renew their password before the expiration day is reached. Once the policies have been created, you must then apply them to the user with the `passwd-policy` entry under the `user local` command. Password policies can be applied to any user (not just local users), however password policies cannot be applied to a user group.

```
config user password-policy
  edit { name }
  # Configure user password policy.
  set name { string } Password policy name. size[35]
  set expire-days { integer } Time in days before the user's password expires. range[0-999]
  set warn-days { integer } Time in days before a password expiration warning message is displayed to the user upon login. range[0-30]
  next
end
```

expire-days <days>

Period of time in days before the user's password expires. Set the value between 0-999. Default is set to 180.

warn-days <days>

Period of time in days before the user is provided a password expiration warning message upon login. Set the value between 0-30. Default is set to 15.

user peer

Use this command to add or edit peer (digital certificate holder) information. Peers that you define can be used in the `vpn ipsec phase1` command if `peertype` is set to `peer`. These peers can also be added to peer groups in the `user peergrp` command. This command refers to certificates imported into the FortiGate unit. You can import CA certificates using the `vpn certificate ca` command and local certificates using the `vpn certificate local` command.

```
config user peer
  edit { name }
    # Configure peer users.
    set name { string } Peer name. size[35]
    set mandatory-ca-verify { enable | disable } Determine what happens to the peer if the CA certificate is not installed. Disable to auto-
    matically consider the peer certificate as valid.
    set ca { string } Name of the CA certificate as returned by the execute vpn certificate ca list command. size[127] - datasource(s): vpn.cer-
    tificate.ca.name
    set subject { string } Peer certificate name constraints. size[255]
    set cn { string } Peer certificate common name. size[255]
    set cn-type { option } Peer certificate common name type.
      string Normal string.
      email Email address.
      FQDN Fully Qualified Domain Name.
      ipv4 IPv4 address.
      ipv6 IPv6 address.
    set ldap-server { string } Name of an LDAP server defined under the user ldap command. Performs client access rights check. size[35] - data-
    source(s): user.ldap.name
    set ldap-username { string } Username for LDAP server bind. size[35]
    set ldap-password { password_string } Password for LDAP server bind. size[128]
    set ldap-mode { password | principal-name } Mode for LDAP peer authentication.
      password Username/password.
      principal-name Principal name.
    set ocspp-override-server { string } Online Certificate Status Protocol (OCSP) server for certificate retrieval. size[35] - datasource(s):
    vpn.certificate.ocsp-server.name
    set two-factor { enable | disable } Enable/disable two-factor authentication, applying certificate and password-based authentication.
    set passwd { password_string } Peer's password used for two-factor authentication. size[128]
  next
end
```

mandatory-ca-verify {enable | disable}

CA certificates installed on the FortiGate unit will check the peer certificate for validity. Enable (by default) or disable to determine what to do if the CA certificate is *not* installed.

- `enable`: Peer will not be authenticated
 - `disable`: Peer certificate is automatically considered valid and authenticated
-

ca <cert-ca>

Name of the CA certificate, as returned by the `execute vpn certificate ca list` command.

subject [constraints]

Optionally, enter any peer certificate name constraints; the name defined here must match the certificate name for successful authentication.

cn <cert-common-name>

Name of the peer certificate common name.

cn-type {string | email | FQDN | ipv4 | ipv6}

Peer certificate common name type.

- `string`: Normal string. This is set by default.
 - `email`: User's email address.
 - `FQDN`: Fully qualified domain name.
 - `ipv4`: User's IPv4 address.
 - `ipv6`: User's IPv6 address.
-

ldap-server <server>

Name of an LDAP server defined under the `user ldap` command. Performs client access rights check for the defined peer.

ldap-username <name>

Login name for the LDAP server.

ldap-password <password>

Login password for the LDAP server.

ldap-mode {password | principal-name}

Mode for LDAP authentication.

- `password`: Authenticate through user name and password. This is set by default.
 - `principal-name`: Authenticate through LDAP `userPrincipalName` attribute.
-

ocsp-override-server <server>

Online Certificate Status Protocol (OCSP) server used to retrieve certificates. This applies if OCSP is enabled in the `vpn certificate setting` command.

two-factor {enable | disable}

Enable or disable (by default) two-factor authentication, applying certificate and password based authentication. Once set, specify the password to use in the `passwd` entry (see entry below).

passwd <password>

Note: This entry is only available when `two-factor` is set to `enable`. This peer's password for two-factor authentication.

user peergrp

Use this command to add or edit peer groups. Peers that you define can be used in the `vpn ipsec phase1` command if `peertype` is set to `peer`.

```
config user peergrp
  edit { name }
  # Configure peer groups.
  set name { string } Peer group name. size[35]
  config member
    edit { name }
    # Peer group members.
    set name { string } Peer group member name. size[35] - datasource(s): user.peer.name
  next
next
end
```

append member <name>

Append peer group members.

member <name>

Member names of the peer group, each separated by a space. To add or remove names from the group, you must re-enter the whole list with the additions or deletions required.

user pop3

Use this command to configure users who authenticate on a Post Office Protocol 3 (POP3) server. Your Internet server uses the POP3 protocol to receive and hold emails.

```
config user pop3
  edit { name }
  # POP3 server entry configuration.
  set name { string }   POP3 server entry name. size[35]
  set server { string } {{ name_str|ip_str }} server domain name or IP. size[63]
  set port { integer }  POP3 service port number. range[0-65535]
  set secure { none | starttls | pop3s }  SSL connection.
    none      None.
    starttls  Use StartTLS.
    pop3s     Use POP3 over SSL.
  next
end
```

server <name/ip>

Domain name or IP address of the POP3 email server.

port <port>

POP3 service port number. This is set to 110 by default).

secure {none | starttls | pop3s}

Security measure to apply: `none`, `starttls` (by default), or `pop3s` (POP3 over SSL).

user radius

Use this command to add or edit information used for RADIUS authentication. The default port for RADIUS traffic is 1812. If your RADIUS server uses a different port you can change the default RADIUS port here. You may set different ports for each of your RADIUS servers, of which you can configure a maximum of ten.

Note: All RADIUS Single-Sign On (RSSO) and other SSO related entries are only available when `rsso` is set to `enable`.

```
config user radius
  edit { name }
  # Configure RADIUS server entries.
  set name { string } RADIUS server entry name. size[35]
  set server { string } Primary RADIUS server CN domain name or IP address. size[63]
  set secret { password_string } Pre-shared secret key used to access the primary RADIUS server. size[128]
  set secondary-server { string } {{ name_str|ip_str }} secondary RADIUS CN domain name or IP. size[63]
  set secondary-secret { password_string } Secret key to access the secondary server. size[128]
  set tertiary-server { string } {{ name_str|ip_str }} tertiary RADIUS CN domain name or IP. size[63]
  set tertiary-secret { password_string } Secret key to access the tertiary server. size[128]
  set timeout { integer } Time in seconds between re-sending authentication requests. range[1-300]
  set all-usergroup { disable | enable } Enable/disable automatically including this RADIUS server in all user groups.
  set use-management-vdom { enable | disable } Enable/disable using management VDOM to send requests.
  set nas-ip { ipv4 address } IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.

  set acct-interim-interval { integer } Time in seconds between each accounting interim update message. range[600-86400]
  set radius-coa { enable | disable } Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.
  set radius-port { integer } RADIUS service port number. range[0-65535]
  set h3c-compatibility { enable | disable } Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.
  set auth-type { option } Authentication methods/protocols permitted for this RADIUS server.
    auto Use PAP, MSCHAP_v2, and CHAP (in that order).
    ms_chap_v2 Microsoft Challenge Handshake Authentication Protocol version 2.
    ms_chap Microsoft Challenge Handshake Authentication Protocol.
    chap Challenge Handshake Authentication Protocol.
    pap Password Authentication Protocol.
  set source-ip { ipv4 address } Source IP address for communications to the RADIUS server.
  set username-case-sensitive { enable | disable } Enable/disable case sensitive user names.
config class
  edit { name }
```

```

# Class attribute name(s).
    set name { string }    Class name. size[64]
next
set password-renewal { enable | disable }    Enable/disable password renewal.
set password-encoding { auto | ISO-8859-1 }    Password encoding.
    auto            Use original password encoding.
    ISO-8859-1    Use ISO-8859-1 password encoding.
set rspo { enable | disable }    Enable/disable RADIUS based single sign on feature.
set rspo-radius-server-port { integer }    UDP port to listen on for RADIUS Start and Stop records. range[0-65535]
set rspo-radius-response { enable | disable }    Enable/disable sending RADIUS response packets after receiving Start and Stop records.
set rspo-validate-request-secret { enable | disable }    Enable/disable validating the RADIUS request shared secret in the Start or End
record.
set rspo-secret { password_string }    RADIUS secret used by the RADIUS accounting server. size[31]
set rspo-endpoint-attribute { option }    RADIUS attributes used to extract the user end point identifier from the RADIUS Start record.
    User-Name            Use this attribute.
    User-Password        Use this attribute.
    CHAP-Password        Use this attribute.
    NAS-IP-Address        Use this attribute.
    NAS-Port            Use this attribute.
    Service-Type        Use this attribute.
    Framed-Protocol        Use this attribute.
    Framed-IP-Address        Use this attribute.
    Framed-IP-Netmask        Use this attribute.
    Framed-Routing        Use this attribute.
    Filter-Id            Use this attribute.
    Framed-MTU            Use this attribute.
    Framed-Compression    Use this attribute.
    Login-IP-Host        Use this attribute.
    Login-Service        Use this attribute.
    Login-TCP-Port        Use this attribute.
    Reply-Message        Use this attribute.
    Callback-Number        Use this attribute.
    Callback-Id            Use this attribute.
    Framed-Route        Use this attribute.
    Framed-IPX-Network    Use this attribute.
    State                Use this attribute.
    Class                Use this attribute.
    Session-Timeout        Use this attribute.
    Idle-Timeout          Use this attribute.
    Termination-Action    Use this attribute.
    Called-Station-Id        Use this attribute.
    Calling-Station-Id        Use this attribute.
    NAS-Identifier        Use this attribute.

```

Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Link	Use this attribute.
Framed-AppleTalk-Network	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Status-Type	Use this attribute.
Acct-Delay-Time	Use this attribute.
Acct-Input-Octets	Use this attribute.
Acct-Output-Octets	Use this attribute.
Acct-Session-Id	Use this attribute.
Acct-Authentic	Use this attribute.
Acct-Session-Time	Use this attribute.
Acct-Input-Packets	Use this attribute.
Acct-Output-Packets	Use this attribute.
Acct-Terminate-Cause	Use this attribute.
Acct-Multi-Session-Id	Use this attribute.
Acct-Link-Count	Use this attribute.
CHAP-Challenge	Use this attribute.
NAS-Port-Type	Use this attribute.
Port-Limit	Use this attribute.
Login-LAT-Port	Use this attribute.

set rso-endpoint-block-attribute { option } RADIUS attributes used to block a user.

User-Name	Use this attribute.
User-Password	Use this attribute.
CHAP-Password	Use this attribute.
NAS-IP-Address	Use this attribute.
NAS-Port	Use this attribute.
Service-Type	Use this attribute.
Framed-Protocol	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Framed-Routing	Use this attribute.
Filter-Id	Use this attribute.
Framed-MTU	Use this attribute.
Framed-Compression	Use this attribute.
Login-IP-Host	Use this attribute.
Login-Service	Use this attribute.
Login-TCP-Port	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.

Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
State	Use this attribute.
Class	Use this attribute.
Session-Timeout	Use this attribute.
Idle-Timeout	Use this attribute.
Termination-Action	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Link	Use this attribute.
Framed-AppleTalk-Network	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Status-Type	Use this attribute.
Acct-Delay-Time	Use this attribute.
Acct-Input-Octets	Use this attribute.
Acct-Output-Octets	Use this attribute.
Acct-Session-Id	Use this attribute.
Acct-Authentic	Use this attribute.
Acct-Session-Time	Use this attribute.
Acct-Input-Packets	Use this attribute.
Acct-Output-Packets	Use this attribute.
Acct-Terminate-Cause	Use this attribute.
Acct-Multi-Session-Id	Use this attribute.
Acct-Link-Count	Use this attribute.
CHAP-Challenge	Use this attribute.
NAS-Port-Type	Use this attribute.
Port-Limit	Use this attribute.
Login-LAT-Port	Use this attribute.
set sso-attribute { option }	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.
User-Name	Use this attribute.
User-Password	Use this attribute.
CHAP-Password	Use this attribute.
NAS-IP-Address	Use this attribute.
NAS-Port	Use this attribute.
Service-Type	Use this attribute.
Framed-Protocol	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.

Framed-Routing	Use this attribute.
Filter-Id	Use this attribute.
Framed-MTU	Use this attribute.
Framed-Compression	Use this attribute.
Login-IP-Host	Use this attribute.
Login-Service	Use this attribute.
Login-TCP-Port	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
State	Use this attribute.
Class	Use this attribute.
Session-Timeout	Use this attribute.
Idle-Timeout	Use this attribute.
Termination-Action	Use this attribute.
Called-Station-Id	Use this attribute.
Calling-Station-Id	Use this attribute.
NAS-Identifier	Use this attribute.
Proxy-State	Use this attribute.
Login-LAT-Service	Use this attribute.
Login-LAT-Node	Use this attribute.
Login-LAT-Group	Use this attribute.
Framed-AppleTalk-Link	Use this attribute.
Framed-AppleTalk-Network	Use this attribute.
Framed-AppleTalk-Zone	Use this attribute.
Acct-Status-Type	Use this attribute.
Acct-Delay-Time	Use this attribute.
Acct-Input-Octets	Use this attribute.
Acct-Output-Octets	Use this attribute.
Acct-Session-Id	Use this attribute.
Acct-Authentic	Use this attribute.
Acct-Session-Time	Use this attribute.
Acct-Input-Packets	Use this attribute.
Acct-Output-Packets	Use this attribute.
Acct-Terminate-Cause	Use this attribute.
Acct-Multi-Session-Id	Use this attribute.
Acct-Link-Count	Use this attribute.
CHAP-Challenge	Use this attribute.
NAS-Port-Type	Use this attribute.
Port-Limit	Use this attribute.
Login-LAT-Port	Use this attribute.

```

    set sso-attribute-key { string } Key prefix for SSO group value in the SSO attribute. size[35]
    set sso-attribute-value-override { enable | disable } Enable/disable override old attribute value with new value for the same endpoint.
    set rso-context-timeout { integer } Time in seconds before the logged out user is removed from the "user context list" of logged on users.
range[0-4294967295]
    set rso-log-period { integer } Time interval in seconds that group event log messages will be generated for dynamic profile events. range
[0-4294967295]
    set rso-log-flags { option } Events to log.
        protocol-error Enable this log type.
        profile-missing Enable this log type.
        accounting-stop-missed Enable this log type.
        accounting-event Enable this log type.
        endpoint-block Enable this log type.
        radiusd-other Enable this log type.
        none Disable all logging.
    set rso-flush-ip-session { enable | disable } Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.
    set rso-ep-one-ip-only { enable | disable } Enable/disable the replacement of old IP addresses with new ones for the same endpoint on
RADIUS accounting Start messages.
    config accounting-server
        edit { id }
            # Additional accounting servers.
            set id { integer } ID (0 - 4294967295). range[0-4294967295]
            set status { enable | disable } Status.
            set server { string } {{ name_str|ip_str }} Server CN domain name or IP. size[63]
            set secret { password_string } Secret key. size[128]
            set port { integer } RADIUS accounting port number. range[0-65535]
            set source-ip { ipv4 address } Source IP address for communications to the RADIUS server.
        next
    next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

server <name/ip>

Note: This entry is only available when `rso` is set to `disable`. RADIUS server domain name or IP address (host name must comply with [RFC1035](#)).

secret <key>

Note: This entry is only available when `rsso` is set to `disable`. RADIUS server shared secret key. The key should be a maximum of 16 characters in length.

timeout <timeout>

Period of time in seconds between re-sending authentication requests. Set the value between 1-300. The default is set to 5. These requests occur during the `remoteauthtimeout` period set in the `system global` command.

all-usergroup {enable | disable}

Note: This entry is only available when `rsso` is set to `disable`. Enable or disable (by default) automatically including this RADIUS server to all user groups.

use-management-vdom {enable | disable}

Note: This entry is only available when `rsso` is set to `disable`. Enable or disable (by default) using the management VDOM to send requests.

nas-ip <ip>

Note: This entry is only available when `rsso` is set to `disable`. IP address of FortiGate interface used to communicate with the RADIUS server, and used as `NAS-IP-Address` and `Called-Station-Id` attribute in RADIUS access requests (see the `rsso-endpoint-attribute` entry below for full list of attributes).

acct-interim-interval <seconds>

Note: This entry is only available when `rsso` is set to `disable`. Period of time in seconds between each accounting interim update message. Set the value between 600-86400 (or ten minutes to one day). The default is set to 0.

radius-coa {enable | disable}

Enable or disable (by default) RADIUS Change of Authorization (CoA), a mechanism that can change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

radius-port <port>

Note: This entry is only available when `rssso` is set to `disable`. RADIUS service port number. Set the value between 0-65535. The default is set to 0.

h3c-compatibility {enable | disable}

Enable or disable (by default) compatibility with the H3C's intelligent Management Center (iMC). When enabled, the supplicant requests 802.1X authentication and then sends a second phase security check request to the H3C IMC server.

auth-type {auto | ms_chap_v2 | ms_chap | chap | pap}

Note: This entry is only available when `rssso` is set to `disable`. Authentication method for this RADIUS server.

- `auto`: Automatic authentication setting, uses `pap`, `ms_chap_v2`, and `chap`. This is set by default.
 - `ms_chap_v2`: MS-CHAPv2
 - `ms_chap`: MS-CHAP
 - `chap`: Challenge-Handshake Authentication Protocol
 - `pap`: Password Authentication Protocol
-

source-ip <ip>

Note: This entry is only available when `rssso` is set to `disable`. Source IP for communications to the RADIUS server.

username-case-sensitive {enable | disable}

Enable or disable (by default) implementation of username case-sensitivity.

class <name>

Class attribute name(s).

password-renewal {enable | disable}

Enable or disable (by default) implementation of password renewal.

rssso {enable | disable}

Enable (or disable by default) RADIUS SSO (RSSO) to set a variety of options and configure an RSSO agent. FortiOS will then accept connections on the port defined in the `rssso-radius-server-port` entry (see entry below).

rssso-radius-server-port <port>

The connection that FortiOS listens for RADIUS Start and Stop records on this port. Set the value between 0-65535. The default is set to 1813. If necessary, change the UDP port number used by the RADIUS accounting server for sending RADIUS records.

rssso-radius-response {enable | disable}

Enable (or disable by default) FortiOS to send RADIUS responses after receiving RADIUS Start and Stop records.

rssso-validate-request-secret {enable | disable}

Enable (or disable by default) FortiOS to verify that the RADIUS secret matches the RADIUS secret in the RADIUS Start or End record. Verifying the RADIUS secret confirms the RADIUS record as valid.

rssso-secret <password>

RADIUS secret used by the RADIUS accounting server.

rsso-endpoint-attribute <attribute>

Note: All attributes listed below are also available under the `rsso-endpoint-block-attribute` and `ssso-attribute` entries. To extract the user end point identifier from the RADIUS Start record, this entry must be set to the name of the RADIUS attribute that contains the end point identifier. The RADIUS attribute must match one of the attributes available. Attributes are case sensitive. The default is set to `Calling-Station-Id``Calling-Station-Id`. Select from the table shown below:

User-Name	Login-IP-Host	Called-Station-Id	Acct-Output-Octets
User-Password	Login-Service	Calling-Station-Id	Acct-Session-Id
CHAP-Password	Login-TCP-Port	NAS-Identifier	Acct-Authentic
NAS-IP-Address	Reply-Message	Proxy-State	Acct-Session-Time
NAS-Port	Callback-Number	Login-LAT-Service	Acct-Input-Packets
Service-Type	Callback-Id	Login-LAT-Node	Acct-Output-Packets
Framed-Protocol	Framed-Route	Login-LAT-Group	Acct-Terminate-Cause
Framed-IP-Address	Framed-IPX-Network	Framed-AppleTalk-Link	Acct-Multi-Session-Id
Framed-IP-Netmask	State	Framed-AppleTalk-Network	Acct-Link-Count
Framed-Routing	Class	Framed-AppleTalk-Zone	CHAP-Challenge
Filter-Id	Session-Timeout	Acct-Status-Type	NAS-Port-Type
Framed-MTU	Idle-Timeout	Acct-Delay-Time	Port-Limit
Framed-Compression	Termination-Action	Acct-Input-Octets	Login-LAT-Port

rsso-endpoint-block-attribute <attribute>

RADIUS attribute used to block a user. See the `rsso-endpoint-attribute` entry for a full list of the attributes available.

sso-attribute <attribute>

Name of the RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record. The default is set to `Class`. See the `radius-endpoint-attribute` entry for a full list of the attributes available.

sso-attribute-key <key>

Key prefix for SSO group value in the SSO attribute, with a maximum length of 36 characters.

sso-attribute-value-override {enable | disable}

Enable (by default) or disable overriding old attribute with a new attribute for the same endpoint.

radius-context-timeout <seconds>

Period of time in seconds before the logged on user is removed from the "user context list" of logged on users. Set the value between 1-4294967295 (or one second to 136+ years), or 0 for users you want to remain on the list. The default is set to 28800 (or eight hours). This timeout is only necessary if FortiOS doesn't receive RADIUS Stop records. However it's advisable to set a timeout in case the FortiGate unit misses a Stop record.

radius-log-period <seconds>

Time interval in seconds that FortiOS will generate group event log messages for dynamic profile events. This is to avoid generating groups of event log messages continuously. Each log message contains the number of events of that type occurred. Set the value between 1-4294967295 (or one second to 136+ years), or 0 (by default) to generate all event log messages in real time.

radius-log-flags {protocol-error | profile-missing | accounting-stop-missed | accounting-event | endpoint-block | radiusd-other | none}

Defines how event log messages are written. Multiple options can be set, each separated by a space.

- `protocol-error`: Writes an event log message if RADIUS protocol errors occur. For example, if a RADIUS record contains a RADIUS secret that does not match the one added to the dynamic profile.

-
- `profile-missing`: Writes an event log message whenever FortiOS cannot find a group name in a RADIUS Start message that matches the name of an RSSO user group in FortiOS.
 - `accounting-stop-missed`: Writes an event log message whenever a user context entry timeout expires indicating that FortiOS removed an entry from the user context list without receiving a RADIUS Stop message.
 - `accounting-event`: Writes an event log message when FortiOS does not find the expected information in a RADIUS Record. For example, if a RADIUS record contains more than the expected number of addresses.
 - `endpoint-block`: Writes an event log message whenever a user is blocked.
 - `radiusd-other`: Writes an event log message for other events. For example, write a log message if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.
 - `none`: Disable logging of RADIUS SSO events.
-

radiusd-ssso-flush-ip-session {enable | disable}

Enable (or disable by default) to flush user IP sessions on RADIUS accounting Stop messages.

radiusd-ssso-ep-one-ip-only {enable | disable}

Enable or disable (by default) the replacement of old IP addresses with new IP addresses for the same endpoint on RADIUS accounting Start messages.

user security-exempt-list

Use this command to define security exempt rules/lists.

Note: To view eligible options for the config options in the entries listed below, enter `set <entry> ?`.

```
config user security-exempt-list
  edit { name }
  # Configure security exemption list.
  set name { string } Name of the exempt list. size[35]
  set description { string } Description. size[127]
  config rule
    edit { id }
    # Configure rules for exempting users from captive portal authentication.
    set id { integer } ID. range[0-4294967295]
    config srcaddr
      edit { name }
      # Source addresses or address groups.
      set name { string } Address or group name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  config devices
    edit { name }
    # Devices or device groups.
    set name { string } Device or group name. size[35] - datasource(s): user.device.alias,user.device-group.name,user.device-
category.name
  next
  config dstaddr
    edit { name }
    # Destination addresses or address groups.
    set name { string } Address or group name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
  config service
    edit { name }
    # Destination services.
    set name { string } Service name. size[64] - datasource(s): firewall.service.custom.name,firewall.service.group.name
  next
next
next
```

end

config rule

A configuration method to create exempt rules. Edit to create new and specify the rule parameters with the entries below.

srcaddr <src-address>

Source addresses or address groups to be exempted from Captive Portal, each separated by a space.

devices <device>

Devices or device groups to be exempted from Captive Portal, each separated by a space. These groups can be created/edited using the `user device-group` command.

dstaddr <dst-address>

Destination addresses or address groups to be exempted from Captive Portal, each separated by a space.

service <dst-service>

Destination services to be exempted from Captive Portal, each separated by a space.

description [description]

Optional description for the group.

user setting

Use this command to configure per VDOM user settings such as the firewall user authentication time out and protocol support for firewall policy authentication.

```
config user setting
  set auth-type { http | https | ftp | telnet } Supported firewall policy authentication protocols/methods.
    http Allow HTTP authentication.
    https Allow HTTPS authentication.
    ftp Allow FTP authentication.
    telnet Allow TELNET authentication.
  set auth-cert { string } HTTPS server certificate for policy authentication. size[35] - datasource(s): vpn.certificate.local.name
  set auth-ca-cert { string } HTTPS CA certificate for policy authentication. size[35] - datasource(s): vpn.certificate.local.name
  set auth-secure-http { enable | disable } Enable/disable redirecting HTTP user authentication to more secure HTTPS.
  set auth-http-basic { enable | disable } Enable/disable use of HTTP basic authentication for identity-based firewall policies.
  set auth-ssl-allow-renegotiation { enable | disable } Allow/forbid SSL re-negotiation for HTTPS authentication.
  set auth-timeout { integer } Time in minutes before the firewall user authentication timeout requires the user to re-authenticate. range[1-1440]
  set auth-timeout-type { idle-timeout | hard-timeout | new-session } Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.
    idle-timeout Idle timeout.
    hard-timeout Hard timeout.
    new-session New session timeout.
  set auth-portal-timeout { integer } Time in minutes before captive portal user have to re-authenticate (1 - 30 min, default 3 min). range[1-30]
  set radius-ses-timeout-act { hard-timeout | ignore-timeout } Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.
    hard-timeout Use session timeout from RADIUS as hard-timeout.
    ignore-timeout Ignore session timeout from RADIUS.
  set auth-blackout-time { integer } Time in seconds an IP address is denied access after failing to authenticate five times within one minute. range[0-3600]
  set auth-invalid-max { integer } Maximum number of failed authentication attempts before the user is blocked. range[1-100]
  set auth-lockout-threshold { integer } Maximum number of failed login attempts before login lockout is triggered. range[1-10]
  set auth-lockout-duration { integer } Lockout period in seconds after too many login failures. range[0-4294967295]
config auth-ports
  edit { id }
  # Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and TELNET.
  set id { integer } ID. range[0-4294967295]
  set type { http | https | ftp | telnet } Service type.
    http HTTP service.
```

```
        https  HTTPS service.
        ftp    FTP service.
        telnet TELNET service.
    set port { integer } Non-standard port for firewall user authentication. range[1-65535]
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

config auth-ports

A configuration method to set authentication ports and their authentication types. Edit to create new and configure the following entries below.

type {http | https | ftp | telnet}

User authentication protocol support for firewall policy authentication for the port. User controls which protocols (HTTP, HTTPS, FTP, and/or TELNET) should support the authentication challenge. The default is set to `http`.

port <port>

Authentication port number. Set the value between 1-65535. The default is set to 1024.

auth-type {http | https | ftp | telnet}

Select the protocols that can be used for firewall policy authentication. Default is `http https ftp telnet`, which means firewall policy authentication can be done using HTTP, HTTPS, FTP or Telnet. You can remove protocols to limit the authentication options.

auth-cert <cert>

HTTPS server certificate for policy authentication. Select from built-in defaults or custom certificates. The built-in `Fortinet_Factory` certificate is set by default.

auth-ca-cert <ca-cert>

If the built-in certificate is not used here, specify the CA certificate to use instead.

auth-secure-http {enable | disable}

Enable or disable (by default) redirecting HTTP user authentication to more secure HTTPS.

auth-http-basic {enable | disable}

Enable or disable (by default) support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of an authentication web page. An example to use this would be for web browsers on mobile devices, as some may only support HTTP basic authentication. Enable or disable (by default) support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of an authentication web page. An example to use this would be for web browsers on mobile devices, as some may only support HTTP basic authentication.

auth-multi-group {enable | disable}

Enable (by default) or disable the retrieval of groups to which a user belongs. You can disable this option if the Active Directory structure is setup such that users belong to only one group.

auth-timeout <minutes>

Period of time in minutes before the firewall user authentication timeout requires the user to authenticate again. Set the value between 1-1440 (or one minute to one day). To improve security, it's recommended to keep the authentication timeout at the default value of 5.

auth-timeout-type {idle-timeout | hard-timeout | new-session}

Type of authentication timeout.

- `idle-timeout`: Applies only to idle sessions. This is set by default.
 - `hard-timeout`: Uses RADIUS timeout.
 - `new-session`: Applies only to new sessions.
-

auth-portal-timeout <minutes>

Period of time in minutes before the firewall Captive Portal authentication timeout requires the user to authenticate again. Set the value between 1-30 (or one minute to half an hour). The default is set to 3.

radius-ses-timeout-act {hard-timeout | ignore-timeout}

RADIUS session timeout action.

- `hard-timeout`: Uses RADIUS timeout. This is set by default.
 - `ignore-timeout`: Ignores RADIUS timeout.
-

auth-blackout-time <seconds>

When a firewall authentication attempt fails five times within one minute, the IP address (that is the source of the authentication attempts) is denied access for this period of time in seconds. Set the value between 0-3600 (or no denial to one hour). The default is set to 0. When a firewall authentication attempt fails five times within one minute, the IP address (that is the source of the authentication attempts) is denied access for this period of time in seconds. Set the value between 0-3600 (or no denial to one hour). The default is set to 0.

auth-invalid-max <failed-attempts>

Maximum number of failed authentication attempts before the client is blocked. Set the value between 1-100. The default is set to 5.

auth-lockout-threshold <login-attempts>

Number of login attempts before a login lockout is triggered. Set the value between 1-10. The default is set to 3.

auth-lockout-duration <seconds>

Period of time in seconds that login lockout lasts for. Set the value between 1-4294967295 (or one second to 136+ years), or 0 for no lockout.

user tacacs+

Use this command to add or edit information used for Terminal Access Controller Access-Control System (TACACS+) authentication, a remote authentication protocol used to communicate with an authentication server. The default port for a TACACS+ server is 49. A maximum of 10 remote TACACS+ servers can be configured, and alternative authentication methods can be set for each server. These methods include CHAP, PAP, MS-CHAP, and ASCII. The host name for TACACS+ servers must comply with [RFC1035](#).

```
config user tacacs+
  edit { name }
  # Configure TACACS+ server entries.
  set name { string } TACACS+ server entry name. size[35]
  set server { string } Primary TACACS+ server CN domain name or IP address. size[63]
  set secondary-server { string } Secondary TACACS+ server CN domain name or IP address. size[63]
  set tertiary-server { string } Tertiary TACACS+ server CN domain name or IP address. size[63]
  set port { integer } Port number of the TACACS+ server. range[1-65535]
  set key { password_string } Key to access the primary server. size[128]
  set secondary-key { password_string } Key to access the secondary server. size[128]
  set tertiary-key { password_string } Key to access the tertiary server. size[128]
  set authen-type { option } Allowed authentication protocols/methods.
    mschap MSCHAP.
    chap CHAP.
    pap PAP.
    ascii ASCII.
    auto Use PAP, MSCHAP, and CHAP (in that order).
  set authorization { enable | disable } Enable/disable TACACS+ authorization.
  set source-ip { ipv4 address } source IP for communications to TACACS+ server.
next
end
```

server <name/ip>

Name or IP address of the TACACS+ sever.

secondary-server <name/ip>

Name or IP address of the second sever.

tertiary-server <name/ip>

Name or IP address of the third sever.

port <port>

TACACS+ port number for this server. Set the value between 1-65535. The default is set to 49.

key <key>

Key used to access the server.

secondary-key <key>

Key used to access the second server.

tertiary-key <key>

Key used to access the third server.

authen-type {mschap | chap | pap | ascii | auto}

Authentication method for this TACACS+ server.

- `mschap`: MS-CHAP
- `chap`: Challenge Handshake Authentication Protocol
- `pap`: Password Authentication Protocol
- `ascii`: American Standard Code for Information Interchange, a protocol that represents characters as numerical values.
- `auto`: Uses PAP, MS-CHAP, and CHAP (in that order). This is set by default.

authorization {enable | disable}

Enable or disable (by default) TACACS+ authorization.

source-ip <src-ip>

Enter the source IP address for communications to the TACACS+ server.

voip

Introduction.

This section includes syntax for the following commands:

- [voip profile](#)

voip profile

Introduction.

```
config voip profile
  edit { name }
  # Configure VoIP profiles.
  set name { string } Profile name. size[35]
  set comment { string } Comment. size[255]
  set status { disable | enable } Enable/disable SIP.
  set rtp { disable | enable } Enable/disable create pinholes for RTP traffic to traverse firewall.
  set open-register-pinhole { disable | enable } Enable/disable open pinhole for REGISTER Contact port.
  set open-contact-pinhole { disable | enable } Enable/disable open pinhole for non-REGISTER Contact port.
  set strict-register { disable | enable } Enable/disable only allow the registrar to connect.
  set register-rate { integer } REGISTER request rate limit (per second, per policy). range[0-4294967295]
  set invite-rate { integer } INVITE request rate limit (per second, per policy). range[0-4294967295]
  set max-dialogs { integer } Maximum number of concurrent calls/dialogs (per policy). range[0-4294967295]
  set max-line-length { integer } Maximum SIP header line length (78-4096). range[78-4096]
  set block-long-lines { disable | enable } Enable/disable block requests with headers exceeding max-line-length.
  set block-unknown { disable | enable } Block unrecognized SIP requests (enabled by default).
  set call-keepalive { integer } Continue tracking calls with no RTP for this many minutes. range[0-10080]
  set block-ack { disable | enable } Enable/disable block ACK requests.
  set block-bye { disable | enable } Enable/disable block BYE requests.
  set block-cancel { disable | enable } Enable/disable block CANCEL requests.
  set block-info { disable | enable } Enable/disable block INFO requests.
  set block-invite { disable | enable } Enable/disable block INVITE requests.
  set block-message { disable | enable } Enable/disable block MESSAGE requests.
  set block-notify { disable | enable } Enable/disable block NOTIFY requests.
  set block-options { disable | enable } Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.
  set block-prack { disable | enable } Enable/disable block prack requests.
  set block-publish { disable | enable } Enable/disable block PUBLISH requests.
  set block-refer { disable | enable } Enable/disable block REFER requests.
  set block-register { disable | enable } Enable/disable block REGISTER requests.
  set block-subscribe { disable | enable } Enable/disable block SUBSCRIBE requests.
  set block-update { disable | enable } Enable/disable block UPDATE requests.
  set register-contact-trace { disable | enable } Enable/disable trace original IP/port within the contact header of REGISTER requests.
  set open-via-pinhole { disable | enable } Enable/disable open pinhole for Via port.
  set open-record-route-pinhole { disable | enable } Enable/disable open pinhole for Record-Route port.
  set rfc2543-branch { disable | enable } Enable/disable support via branch compliant with RFC 2543.
```

```

set log-violations { disable | enable } Enable/disable logging of SIP violations.
set log-call-summary { disable | enable } Enable/disable logging of SIP call summary.
set nat-trace { disable | enable } Enable/disable preservation of original IP in SDP i line.
set subscribe-rate { integer } SUBSCRIBE request rate limit (per second, per policy). range[0-4294967295]
set message-rate { integer } MESSAGE request rate limit (per second, per policy). range[0-4294967295]
set notify-rate { integer } NOTIFY request rate limit (per second, per policy). range[0-4294967295]
set refer-rate { integer } REFER request rate limit (per second, per policy). range[0-4294967295]
set update-rate { integer } UPDATE request rate limit (per second, per policy). range[0-4294967295]
set options-rate { integer } OPTIONS request rate limit (per second, per policy). range[0-4294967295]
set ack-rate { integer } ACK request rate limit (per second, per policy). range[0-4294967295]
set prack-rate { integer } PRACK request rate limit (per second, per policy). range[0-4294967295]
set info-rate { integer } INFO request rate limit (per second, per policy). range[0-4294967295]
set publish-rate { integer } PUBLISH request rate limit (per second, per policy). range[0-4294967295]
set bye-rate { integer } BYE request rate limit (per second, per policy). range[0-4294967295]
set cancel-rate { integer } CANCEL request rate limit (per second, per policy). range[0-4294967295]
set preserve-override { disable | enable } Override i line to preserve original IPS (default: append).
set no-sdp-fixup { disable | enable } Enable/disable no SDP fix-up.
set contact-fixup { disable | enable } Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.
set max-idle-dialogs { integer } Maximum number established but idle dialogs to retain (per policy). range[0-4294967295]
set block-geo-red-options { disable | enable } Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.
set hosted-nat-traversal { disable | enable } Hosted NAT Traversal (HNT).
set hnt-restrict-source-ip { disable | enable } Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is
enabled.

set max-body-length { integer } Maximum SIP message body length (0 meaning no limit). range[0-4294967295]
set unknown-header { discard | pass | respond } Action for unknown SIP header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-request-line { discard | pass | respond } Action for malformed request line.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-via { discard | pass | respond } Action for malformed VIA header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-from { discard | pass | respond } Action for malformed From header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-to { discard | pass | respond } Action for malformed To header.
    discard Discard malformed messages.
    pass Bypass malformed messages.

```

```
        respond Respond with error code.
set malformed-header-call-id { discard | pass | respond } Action for malformed Call-ID header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-cseq { discard | pass | respond } Action for malformed CSeq header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-rack { discard | pass | respond } Action for malformed RACK header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-rseq { discard | pass | respond } Action for malformed RSeq header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-contact { discard | pass | respond } Action for malformed Contact header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-record-route { discard | pass | respond } Action for malformed Record-Route header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-route { discard | pass | respond } Action for malformed Route header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-expires { discard | pass | respond } Action for malformed Expires header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-content-type { discard | pass | respond } Action for malformed Content-Type header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-content-length { discard | pass | respond } Action for malformed Content-Length header.
    discard Discard malformed messages.
    pass Bypass malformed messages.
    respond Respond with error code.
set malformed-header-max-forwards { discard | pass | respond } Action for malformed Max-Forwards header.
    discard Discard malformed messages.
```

```

    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-allow { discard | pass | respond } Action for malformed Allow header.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-p-asserted-identity { discard | pass | respond } Action for malformed P-Asserted-Identity header.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-v { discard | pass | respond } Action for malformed SDP v line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-o { discard | pass | respond } Action for malformed SDP o line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-s { discard | pass | respond } Action for malformed SDP s line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-i { discard | pass | respond } Action for malformed SDP i line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-c { discard | pass | respond } Action for malformed SDP c line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-b { discard | pass | respond } Action for malformed SDP b line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-z { discard | pass | respond } Action for malformed SDP z line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-k { discard | pass | respond } Action for malformed SDP k line.
    discard Discard malformed messages.
    pass    Bypass malformed messages.
    respond Respond with error code.
set malformed-header-sdp-a { discard | pass | respond } Action for malformed SDP a line.

```

```

        discard Discard malformed messages.
        pass Bypass malformed messages.
        respond Respond with error code.
set malformed-header-sdp-t { discard | pass | respond } Action for malformed SDP t line.
        discard Discard malformed messages.
        pass Bypass malformed messages.
        respond Respond with error code.
set malformed-header-sdp-r { discard | pass | respond } Action for malformed SDP r line.
        discard Discard malformed messages.
        pass Bypass malformed messages.
        respond Respond with error code.
set malformed-header-sdp-m { discard | pass | respond } Action for malformed SDP m line.
        discard Discard malformed messages.
        pass Bypass malformed messages.
        respond Respond with error code.
set provisional-invite-expiry-time { integer } Expiry time for provisional INVITE (10 - 3600 sec). range[10-3600]
set ips-rtsp { disable | enable } Enable/disable allow IPS on RTP.
set ssl-mode { off | full } SSL/TLS mode for encryption & decryption of traffic.
        off No SSL.
        full Client to FortiGate and FortiGate to Server SSL.
set ssl-send-empty-frags { enable | disable } Send empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).
set ssl-client-renegotiation { allow | deny | secure } Allow/block client renegotiation by server.
        allow Allow a SSL client to renegotiate.
        deny Abort any SSL connection that attempts to renegotiate.
        secure Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.
set ssl-algorithm { high | medium | low } Relative strength of encryption algorithms accepted in negotiation.
        high High encryption. Allow only AES and ChaCha.
        medium Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
        low Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
set ssl-pfs { require | deny | allow } SSL Perfect Forward Secrecy.
        require PFS mandatory.
        deny PFS rejected.
        allow PFS allowed.
set ssl-min-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 } Lowest SSL/TLS version to negotiate.
        ssl-3.0 SSL 3.0.
        tls-1.0 TLS 1.0.
        tls-1.1 TLS 1.1.
        tls-1.2 TLS 1.2.
set ssl-max-version { ssl-3.0 | tls-1.0 | tls-1.1 | tls-1.2 } Highest SSL/TLS version to negotiate.
        ssl-3.0 SSL 3.0.
        tls-1.0 TLS 1.0.
        tls-1.1 TLS 1.1.
        tls-1.2 TLS 1.2.

```

```
        set ssl-client-certificate { string } Name of Certificate to offer to server if requested. size[35] - datasource(s): vpn.cer-
tificate.local.name
        set ssl-server-certificate { string } Name of Certificate return to the client in every SSL connection. size[35] - datasource(s):
vpn.certificate.local.name
        set ssl-auth-client { string } Require a client certificate and authenticate it with the peer/peergrp. size[35] - datasource(s): user-
.peer.name,user.peergrp.name
        set ssl-auth-server { string } Authenticate the server's certificate with the peer/peergrp. size[35] - datasource(s):
user.peer.name,user.peergrp.name
        set status { disable | enable } Enable/disable SCCP.
        set block-mcast { disable | enable } Enable/disable block multicast RTP connections.
        set verify-header { disable | enable } Enable/disable verify SCCP header content.
        set log-call-summary { disable | enable } Enable/disable log summary of SCCP calls.
        set log-violations { disable | enable } Enable/disable logging of SCCP violations.
        set max-calls { integer } Maximum calls per minute per SCCP client (max 65535). range[0-65535]
    next
end
```

vpn

Use `vpn` commands to configure options related to virtual private networking through the FortiGate unit, including:

- IPsec operating parameters
- a local address range for PPTP or L2TP clients
- SSL VPN configuration settings

This section includes syntax for the following commands:

- `vpn certificate ca`
- `vpn certificate cri`
- `vpn certificate local`
- `vpn certificate ocsip-server`
- `vpn certificate remote`
- `vpn certificate setting`
- `vpn ipsec concentrator`
- `vpn ipsec forticlient`
- `vpn ipsec manualkey-interface | manualkey`
- `vpn ipsec phase1-interface | phase1`
- `vpn ipsec phase2-interface | phase2`
- `vpn l2tp`
- `vpn pptp`
- `vpn ssl settings`
- `vpn ssl web host-check-software`
- `vpn ssl web portal`
- `vpn ssl web realm`
- `vpn ssl web user-bookmark`
- `vpn ssl web user-group-bookmark`
- `vpn ssl web virtual-desktop-app-list`

vpn certificate ca

Use this command to install Certificate Authority (CA) root certificates. When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the CRL.

```
config vpn certificate ca
  edit { name }
  # CA certificate.
  set name { string } Name. size[79]
  set ca { string } CA certificate as a PEM file.
  set range { global | vdom } Either global or VDOM IP address range for the CA certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } CA certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  set trusted { enable | disable } Enable/disable as a trusted CA.
  set scep-url { string } URL of the SCEP server. size[255]
  set auto-update-days { integer } Number of days to wait before requesting an updated CA certificate (0 - 4294967295, 0 = disabled). range
[0-4294967295]
  set auto-update-days-warning { integer } Number of days before an expiry-warning message is generated (0 - 4294967295, 0 = disabled). range
[0-4294967295]
  set source-ip { ipv4 address } Source IP address for communications to the SCEP server.
  set last-updated { integer } Time at which CA was last updated. range[0-4294967295]
  next
end
```

ca <cert>

Enter or retrieve the CA certificate as a Privacy Enhanced Mail (PEM) file.

range {global | vdom}

Either `global` (by default) or `vdom` IP address range for the CA certificate.

source {factory | user | bundle | fortiguard}

CA certificate source.

- **factory:** Default certificate that came with the FortiGate
 - **user:** User certificate (set by default)
 - **bundle:** Certificate from a bundle file
 - **fortiguard:** Certificate from FortiGuard
-

trusted {enable | disable}

Enable (by default) or disable as a trusted CA.

scep-url <url>

URL of the Simple Certificate Enrollment Protocol (SCEP) server.

auto-update-days <days>

Note: This entry is only available when `scep-url` has been set. Amount of time in days before the FortiGate requests an updated CA certificate. Set to 0 (by default) for no auto-update.

auto-update-days-warning <days>

Note: This entry is only available when `scep-url` has been set. Amount of time in days before the FortiGate generates an expiry-warning message. Set to 0 (by default) for no warning.

source-ip <ipv4-address>

IPv4 address used to verify that the request is sent from an expected IP.

vpn certificate crl

Use this command to install a Certificate Revocation List (CRL). When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the CRL.

```
config vpn certificate crl
  edit { name }
  # Certificate Revocation List as a PEM file.
  set name { string } Name. size[35]
  set crl { string } Certificate Revocation List as a PEM file.
  set range { global | vdom } Either global or VDOM IP address range for the certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } Certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  set update-vdom { string } VDOM for CRL update. size[31] - datasource(s): system.vdom.name
  set ldap-server { string } LDAP server name for CRL auto-update. size[35]
  set ldap-username { string } LDAP server user name. size[63]
  set ldap-password { password_string } LDAP server user password. size[128]
  set http-url { string } HTTP server URL for CRL auto-update. size[255]
  set scep-url { string } SCEP server URL for CRL auto-update. size[255]
  set scep-cert { string } Local certificate for SCEP communication for CRL auto-update. size[35] - datasource(s): vpn.certificate.local.name
  set update-interval { integer } Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.
range[0-4294967295]
  set source-ip { ipv4 address } Source IP address for communications to a HTTP or SCEP CA server.
  set last-updated { integer } Time at which CRL was last updated. range[0-4294967295]
  next
end
```

crl <pem-file>

The name of the CRL in Privacy Enhanced Mail (PEM) format.

range {global | vdom}

Either `global` (by default) or `vdom` IP address range for the certificate.

source {factory | user | bundle | fortiguard}

CA certificate source.

- **factory:** Default certificate that came with the FortiGate
 - **user:** User certificate (set by default)
 - **bundle:** Certificate from a bundle file
 - **fortiguard:** Certificate from FortiGuard
-

update-vdom <vdom>

Name of the VDOM for CRL update. This is set to the `root` VDOM by default.

ldap-server <name>

Name of the LDAP server defined in `config user ldap` for CRL auto-update.

ldap-username <name>

Note: This entry is only available when `ldap-server` has been set. LDAP login name.

ldap-password <password>

Note: This entry is only available when `ldap-server` has been set. LDAP login password.

http-url <url>

URL of an HTTP server used for automatic CRL certificate updates. The URL *must* begin with either **http://** or **https://**.

scep-url <url>

URL of the SCEP server used for automatic CRL certificate updates. The URL *must* begin with either **http://** or **https://**.

scep-cert <cert>

Local certificate used for SCEP communication for CRL auto-update. If a certificate hasn't already been set, the default certificate used is `Fortinet_CA_SSL`.

update-interval <interval>

Period of time in seconds before the FortiGate unit checks for an updated CRL. Enter 0 (by default) to update the CRL only when it expires.

source-ip <ipv4-address>

IPv4 address used to verify that the request is sent from an expected IP.

vpn certificate local

Use this command to install local certificates.

```
config vpn certificate local
  edit { name }
  # Local keys and certificates.
  set name { string } Name. size[35]
  set password { password_string } Password as a PEM file. size[128]
  set comments { string } Comment. size[511]
  set private-key { string } PEM format key, encrypted with a password.
  set certificate { string } PEM format certificate.
  set csr { string } Certificate Signing Request.
  set state { string } Certificate Signing Request State.
  set scep-url { string } SCEP server URL. size[255]
  set range { global | vdom } Either a global or VDOM IP address range for the certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } Certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  set auto-regenerate-days { integer } Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).
range[0-4294967295]
  set auto-regenerate-days-warning { integer } Number of days to wait before an expiry warning message is generated (0 = disabled). range[0-
4294967295]
  set scep-password { password_string } SCEP server challenge password for auto-regeneration. size[128]
  set ca-identifier { string } CA identifier of the CA server for signing via SCEP. size[255]
  set name-encoding { printable | utf8 } Name encoding method for auto-regeneration.
    printable Printable encoding (default).
    utf8 UTF-8 encoding.
  set source-ip { ipv4 address } Source IP address for communications to the SCEP server.
  set ike-localid { string } Local ID the FortiGate uses for authentication as a VPN client. size[63]
  set ike-localid-type { asn1dn | fqdn } IKE local ID type.
    asn1dn ASN.1 distinguished name.
    fqdn Fully qualified domain name.
  set last-updated { integer } Time at which certificate was last updated. range[0-4294967295]
next
```

end

password <password>

Password in Privacy Enhanced Mail (PEM) format.

comments [string]

Optional comments.

private-key <key>

Private key in PEM format, encrypted with the password.

certificate <certificate>

Note: This is only available for local entries that have certificates assigned to them already. Certificate in PEM format.

scep-url <url>

URL for the Simple Certificate Enrollment Protocol (SCEP) server.

range {global | vdom}

Either `global` (by default) or `vdom` IP address range for the certificate.

source {factory | user | bundle | fortiguard}

Select the certificate's source:

- **factory:** Default certificate that came with the FortiGate
 - **user:** User certificate (set by default)
-

- **bundle:** Certificate from a bundle file
- **fortiguard:** Certificate from FortiGuard

auto-regenerate-days <days>

Note: This entry is only available when `scep-url` has been set. Number of days before expiry that the FortiGate requests an updated local certificate. Set to 0 (by default) for no auto-update.

auto-regenerate-days-warning <days>

Note: This entry is only available when `scep-url` has been set. Number of days before expiry that the FortiGate generates an expiry-warning message. Set to 0 (by default) for no warning.

scep-password <password>

Note: This entry is only available when `scep-url` has been set. Password for the SCEP server.

ca-identifer <name>

Note: This entry is only available when `scep-url` has been set. CA identifier of the CA server for signing via SCEP.

name-encoding {printable | utf8}

Note: This entry is only available when `scep-url` has been set. Name encoding method for auto-regeneration:

- **printable:** Printable encoding (also known as Quoted-Printable, or QP encoding) uses printable ASCII alphanumeric characters and the equals (=) sign (set by default).
- **utf8:** UTF-8 encoding uses all possible characters.

source-ip <ipv4-addr>

Source IP address for communications to the SCEP server.

ike-localid <id>

Note: This entry is only available when `ike-localid-type` is set to `fqdn`. Local ID that the FortiGate will use for authentication purposes as a VPN client.

ike-localid-type <type>

IKE local ID type:

- **asn1dn:** ASN.1 Distinguished Name ID (set by default)
- **fqdn:** Fully Qualified Domain Name ID

vpn certificate ocsip-server

Use this command to specify the revocation for an Online Certificate Status Protocol (OCSP) server certificate. You can also specify the action to take if the server is not available.

```
config vpn certificate ocsip-server
  edit { name }
  # OCSP server configuration.
  set name { string }   OCSP server entry name. size[35]
  set url { string }   OCSP server URL. size[127]
  set cert { string }   OCSP server certificate. size[127] - datasource(s): vpn.certificate.remote.name,vpn.certificate.ca.name
  set secondary-url { string }   Secondary OCSP server URL. size[127]
  set secondary-cert { string }   Secondary OCSP server certificate. size[127] - datasource(s): vpn.cer-
tificate.remote.name,vpn.certificate.ca.name
  set unavail-action { revoke | ignore }   Action when server is unavailable (revoke the certificate or ignore the result of the check).
    revoke   Revoke certificate if server is unavailable.
    ignore   Ignore OCSP check if server is unavailable.
  set source-ip { ipv4 address }   Source IP address for communications to the OCSP server.
  next
end
```

url <ocsp-url>

URL of the OCSP server.

cert <name>

The OCSP server public certificate (one of the remote certificates).

secondary-url <url>

Secondary URL of the OCSP server.

secondary-cert <name>

Secondary public certificate of the OCSP server (one of the remote certificates).

unavail-action {revoke | ignore}

Upon client certification, when the server is *unreachable*, either `revoke` (by default) the certificate or `ignore` OCSP check.

source-ip <ipv4-address>

Source IP address for communications to the OCSP server.

vpn certificate remote

Use this command to install remote certificates and configure basic settings. The remote certificates are public certificates without a private key, and used as OCSF server certificates.

```
config vpn certificate remote
  edit { name }
  # Remote certificate as a PEM file.
  set name { string } Name. size[35]
  set remote { string } Remote certificate.
  set range { global | vdom } Either the global or VDOM IP address range for the remote certificate.
    global Global range.
    vdom VDOM IP address range.
  set source { factory | user | bundle | fortiguard } Remote certificate source type.
    factory Factory installed certificate.
    user User generated certificate.
    bundle Bundle file certificate.
    fortiguard FortiGuard generated certificate.
  next
end
```

remote <cert>

Name of the remote certificate, in PEM format.

range {global | vdom}

Either `global` (by default) or `vdom` IP address range for the certificate.

source {factory | user | bundle | fortiguard}

Select the certificate's source:

-
- **factory:** Default certificate that came with the FortiGate
 - **user:** User certificate (set by default)
 - **bundle:** Certificate from a bundle file
 - **fortiguard:** Certificate from FortiGuard

vpn certificate setting

Use this command to enable receiving certificates by OCSP.

```
config vpn certificate setting
  set ocsdp-status { enable | disable } Enable/disable receiving certificates using the OCSP.
  set ssl-ocsp-status { enable | disable } Enable/disable SSL OCSP.
  set ssl-ocsp-option { certificate | server } Specify whether the OCSP URL is from the certificate or the
  default OCSP server.
    certificate Use URL from certificate.
    server Use URL from default OCSP server.
  set ocsdp-default-server { string } Default OCSP server. size[35] - datasource(s): vpn.certificate.ocsdp-
  server.name
  set check-ca-cert { enable | disable } Enable to check the CA certificate and fail authentication if cer-
  tificate is not found.
  set subject-match { substring | value } When searching for a matching certificate, control how to find
  matches in the certificate subject name.
    substring Find a match if any string in the certificate subject name matches the name being
    searched for.
    value Find a match if any attribute value string in a certificate subject name is an exact
    match with the name being searched for.
  set cn-match { substring | value } When searching for a matching certificate, control how to find matches
  in the cn attribute of the certificate subject name.
    substring Find a match if any string in a certificate subject name cn attribute name matches the
    name being searched for.
    value Find a match if the cn attribute value string is an exact match with the name being
    searched for.
  set strict-crl-check { enable | disable } Enable/disable strict mode CRL checking.
  set strict-ocsp-check { enable | disable } Enable/disable strict mode OCSP checking.
  set certname-rsa1024 { string } 1024 bit RSA key certificate for re-signing server certificates for SSL
  inspection. size[35] - datasource(s): vpn.certificate.local.name
  set certname-rsa2048 { string } 2048 bit RSA key certificate for re-signing server certificates for SSL
  inspection. size[35] - datasource(s): vpn.certificate.local.name
  set certname-dsa1024 { string } 1024 bit DSA key certificate for re-signing server certificates for SSL
```

```
inspection. size[35] - datasource(s): vpn.certificate.local.name
    set certname-dsa2048 { string } 2048 bit DSA key certificate for re-signing server certificates for SSL
inspection. size[35] - datasource(s): vpn.certificate.local.name
    set certname-ecdsa256 { string } 256 bit ECDSA key certificate for re-signing server certificates for SSL
inspection. size[35] - datasource(s): vpn.certificate.local.name
    set certname-ecdsa384 { string } 384 bit ECDSA key certificate for re-signing server certificates for SSL
inspection. size[35] - datasource(s): vpn.certificate.local.name
end
```

Supplemental Information

The following section is for those commands that require further explanation.

ocsp-status {enable | disable}

Enable or disable (by default) receiving the certificates using the OCSP.

ocsp-default-server <server>

The OCSP server to be used by default. This is one of the servers defined in `config vpn certificate ocsp-server`.

check-ca-cert {enable | disable}

Enable (by default) to check the CA certificate and fail the authentication if the certificate is not found.

strict-crl-check {enable | disable}

Enable or disable (by default) strict mode certificate revocation list (CRL) checking. If strict checking is *not* enabled and a certificate is found to be on a CRL list, the certificate can be used, but a warning log message is written. If strict checking is enabled then all authentication actions that use this certificate fail in addition to the warning message being written.

strict-ocsp-check {enable | disable}

Enable or disable (by default) strict mode OCSP checking. If strict checking is *not* enabled and an OCSP server responds with `cert status unknown`, the certificate can be used, but a warning log message is written. If strict checking is enabled then all authentication actions that use this certificate fail in addition to the warning message being written.

vpn ipsec concentrator

In a hub-and-spoke network, policy-based VPN connections to a number of remote peers radiate from a single, central FortiGate unit, or "hub". The hub functions as a concentrator on the network, managing all VPN connections between the peers, or "spokes". VPN traffic passes from one tunnel to the other through the hub. Add IPsec policy-based VPN tunnels to a VPN concentrator, allowing VPN traffic to pass from one tunnel to the other through the FortiGate unit.

Note: VPN concentrators are only available in NAT/Route mode.

```
config vpn ipsec concentrator
  edit { name }
  # Concentrator configuration.
  set name { string }   Concentrator name. size[35]
  set src-check { disable | enable }   Enable to check source address of phase 2 selector. Disable to check only the destination selector.
  config member
    edit { name }
    # Names of up to 3 VPN tunnels to add to the concentrator.
    set name { string }   Member name. size[64] - datasource(s): vpn.ipsec.manualkey.name,vpn.ipsec.phase1.name
  next
next
end
```

src-check {enable | disable}

Enable to check the source address of the phase 2 selector when locating the best matching phase 2 in a concentrator. Disable (by default) to check only the destination selector.

member <name> [name] [name]

Enter the names of up to three VPN tunnels to add to the concentrator, each separated by a space. Members can be tunnels defined in `vpn ipsec phase1` or `vpn ipsec manualkey`.

vpn ipsec forticlient

Configure automatic VPN connection for FortiClient users. FortiClient users who wish to use automatic VPN configuration must be members of a user group. The command below creates a realm that associates the user group with phase 2 VPN configurations.

```
config vpn ipsec forticlient
  edit { realm }
  # Configure FortiClient policy realm.
  set realm { string } FortiClient realm name. size[35]
  set usergroupname { string } User group name for FortiClient users. size[35] - datasource(s): user.group.name
  set phase2name { string } Phase 2 tunnel name that you defined in the FortiClient dialup configuration. size[35] - datasource(s):
  vpn.ipsec.phase2.name,vpn.ipsec.phase2-interface.name
  set status { enable | disable } Enable/disable this FortiClient configuration.
  next
end
```

usergroupname <name>

Enter the name of a pre-existing user group created for dialup clients.

phase2name <name>

Enter the name of the pre-existing phase 2 tunnel configuration defined for the dialup-client configuration.

status {enable | disable}

Enable (by default) or disable IPsec VPN policy distribution.

vpn ipsec {manualkey-interface | manualkey}

Use `manualkey-interface` to configure manual keys for a route-based (interface mode) IPsec VPN tunnel. Creating a route-based tunnel automatically creates a virtual IPsec interface on the FortiGate unit. This interface can be modified afterward using the system network interface command, however this command is only available in NAT/Route mode.

You can also use `manualkey` to configure manual keys for IPsec tunnel-mode VPN tunnels that connect a FortiGate unit and a remote client or gateway that is also using manual key. Because the keys are created when you configure the tunnel, no negotiation is required for the VPN tunnel to start. However, the remote client or gateway must use the same encryption and authentication algorithms and keys.

Note: To avoid confusion, the various similar authentication and encryption entries vary in availability, depending on which command is used. Among others, the following authentication/encryption entries are *not* available under the `manualkey` command:

- `auth-alg`
- `enc-alg`
- `auth-key`
- `enc-key`
- `local-spi`
- `remote-spi`

```
config vpn ipsec manualkey-interface
  edit { name }
    # Configure IPsec manual keys.
    set name { string }    IPsec tunnel name. size[15]
    set interface { string }  Name of the physical, aggregate, or VLAN interface. size[15] - datasource(s): system.interface.name
    set ip-version { 4 | 6 }  IP version to use for VPN interface.
        4 Use IPv4 addressing for gateways.
        6 Use IPv6 addressing for gateways.
    set addr-type { 4 | 6 }  IP version to use for IP packets.
        4 Use IPv4 addressing for IP packets.
        6 Use IPv6 addressing for IP packets.
    set remote-gw { ipv4 address }  IPv4 address of the remote gateway's external interface.
    set remote-gw6 { ipv6 address }  Remote IPv6 address of VPN gateway.
    set local-gw { ipv4 address any }  IPv4 address of the local gateway's external interface.
    set local-gw6 { ipv6 address }  Local IPv6 address of VPN gateway.
    set auth-alg { option }  Authentication algorithm. Must be the same for both ends of the tunnel.
```

```

        null    null
        md5     md5
        sha1    sha1
        sha256  sha256
        sha384  sha384
        sha512  sha512
    set enc-alg { option }  Encryption algorithm. Must be the same for both ends of the tunnel.
        null    null
        des     des
        3des    3des
        aes128  aes128
        aes192  aes192
        aes256  aes256
        arial28 arial28
        arial92 arial92
        aria256 aria256
        seed    seed
    set auth-key { string }  Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.
    set enc-key { string }   Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.
    set local-spi { string } Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption
rules.
    set remote-spi { string } Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption
rules.
    set npu-offload { enable | disable }  Enable/disable offloading IPsec VPN manual key sessions to NPUs.
    next
end

config vpn ipsec manualkey
    edit { name }
        # Configure IPsec manual keys.
        set name { string }  IPsec tunnel name. size[35]
        set interface { string }  Name of the physical, aggregate, or VLAN interface. size[15] - datasource(s): system.interface.name
        set remote-gw { ipv4 address }  Peer gateway.
        set local-gw { ipv4 address any }  Local gateway.
        set authentication { option }  Authentication algorithm. Must be the same for both ends of the tunnel.
            null    Null.
            md5     MD5.
            sha1    SHA1.
            sha256  SHA256.
            sha384  SHA384.
            sha512  SHA512.
        set encryption { option }  Encryption algorithm. Must be the same for both ends of the tunnel.

```

```
    null      Null.
    des       DES.
    3des      3DES.
    aes128    AES128.
    aes192    AES192.
    aes256    AES256.
    arial28   ARIA128.
    arial92   ARIA192.
    aria256   ARIA256.
    seed      Seed.
set authkey { string }   Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.
set enckey { string }    Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.
set localspi { string }  Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption
rules.
set remotespi { string } Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption
rules.
set npu-offload { enable | disable }  Enable/disable NPU offloading.
  next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

interface <name>

The name of the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.

ip-version {4 | 6}

Enter 4 (by default) for IPv4 or 6 for IPv6 encapsulation for gateways.

addr-type {4 | 6}

Enter 4 (by default) for IPv4 or 6 for IPv6 encapsulation for IP packets.

remote-gw <ip-addr>

The IP address of the remote gateway's external interface.

local-gw [sec-ip-addr]

An optional secondary IP address of the interface selected in the `interface` entry used for the local end of the VPN tunnel.

auth-alg <algorithm>

Enter one of the following authentication algorithms:

- `null`
- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

Make sure to use the same algorithm at both ends of the tunnel.

Note: The `auth-alg` and `enc-alg` entries cannot both be `null`.

enc-alg <algorithm>

Enter one of the following encryption algorithms:

- `null`
- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.

- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.
- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA algorithm may not be available on some FortiGate models. Make sure to use the same algorithm at both ends of the tunnel.

Note: The `auth-alg` and `enc-alg` entries cannot both be `null`.

auth-key <key>

Note: This entry is only available when `auth-alg` is set to either `md5`, `sha1`, or `sha256`. The authentication key in 16-digit (8-byte) segments separated by hyphens. For an MD5 key, enter a 32-digit (16-byte) hexadecimal number: eg: 0102030405060708-090a0b0c0d0e0f10

- For a SHA1 key, enter a 40-digit (20-byte) hexadecimal number. The final segment is only 8-digits (4-bytes).
- For a SHA256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

enc-key <key>

Note: This entry is only available when `enc-alg` is set to either `des`, `3des`, `aes128`, `aes192`, or `aes256`. The encryption key in 16-digit (8-byte) segments separated by hyphens.

- For a DES key, enter a 16-digit (8-byte) hexadecimal number.
- For a 3DES key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES128 key, enter a 32-digit (16-byte) hexadecimal number.
- For an AES192 key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

local-spi <hex-number>

The local Security Parameter Index (SPI), a tag that helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the remote SPI at the opposite end of the tunnel.

remote-spi <hex-number>

The remote SPI. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the local SPI at the opposite end of the tunnel.

authentication <algorithm>

Enter one of the following authentication algorithms:

- `null`
- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

Make sure to use the same algorithm at both ends of the tunnel.

Note: The `authentication` and `encryption` entries cannot both be `null`.

encryption <algorithm>

Enter one of the following encryption algorithms:

- `null`
- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.

- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA and seed algorithms may not be available on some FortiGate models. Make sure to use the same algorithm at both ends of the tunnel.

Note: The `authentication` and `encryption` entries cannot both be `null`.

authkey <key>

Note: This entry is only available when `authentication` is set to either `md5`, `sha1`, or `sha256`. The authentication key in 16-digit (8-byte) segments separated by hyphens. For an MD5 key, enter a 32-digit (16-byte) hexadecimal number: eg: `0102030405060708-090a0b0c0d0e0f10`

- For a SHA1 key, enter a 40-digit (20-byte) hexadecimal number. The final segment is only 8-digits (4-bytes).
- For a SHA256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

enckey <key>

Note: This entry is only available when `encryption` is set to either `des`, `3des`, `aes128`, `aes192`, or `aes256`. The encryption key in 16-digit (8-byte) segments separated by hyphens.

- For a DES key, enter a 16-digit (8-byte) hexadecimal number.
- For a 3DES key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES128 key, enter a 32-digit (16-byte) hexadecimal number.
- For an AES192 key, enter a 48-digit (24-byte) hexadecimal number.
- For an AES256 key, enter a 64-digit (32-byte) hexadecimal number.

Digits can range between 0-9 and a-f. Make sure to use the same key at both ends of the tunnel.

localspi <hex-number>

The local Security Parameter Index (SPI), a tag that helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the remote SPI at the opposite end of the tunnel.

remotespi <hex-number>

The remote SPI. Enter an 8-digit (4-byte) hexadecimal number in the range of 100 to FFFFFFFF. This number must be added to the local SPI at the opposite end of the tunnel.

npu-offload {enable | disable}

Enable (by default) or disable offloading of VPN session to a network processing unit (NPU).

vpn ipsec {phase1-interface | phase1}

Use `phase1-interface` to define a phase 1 definition for a route-based (interface mode) IPsec VPN tunnel that generates authentication and encryption keys automatically. Optionally, you can create a route-based phase 1 definition to act as a backup for another IPsec interface; this is achieved with the `set monitor <phase1>` entry below.

You can also use `phase1` to add or edit IPsec tunnel-mode phase 1 configurations, which define how the FortiGate unit and a remote VPN peer (gateway or client) authenticate themselves to each other as part of establishing the IPsec VPN tunnel.

Note: Some entries are *not* available under the `phase1` command, including the following:

- `ip-version`
- `local-gw6`
- `remote-gw6`
- `monitor` (and all other monitor related entries)
- `add-gw-route`
- `auto-discovery-sender` (and all other auto discovery related entries)
- `encapsulation` (and all other encapsulation related entries)
- `childless-ike`

```
config vpn ipsec phase1-interface
edit { name }
# Configure VPN remote gateway.
set name { string } IPsec remote gateway name. size[15]
set type { static | dynamic | ddns } Remote gateway type.
    static Remote VPN gateway has fixed IP address.
    dynamic Remote VPN gateway has dynamic IP address.
    ddns Remote VPN gateway has dynamic IP address and is a dynamic DNS client.
set interface { string } Local physical, aggregate, or VLAN outgoing interface. size[35] - datasource(s): system.interface.name
set ip-version { 4 | 6 } IP version to use for VPN interface.
    4 Use IPv4 addressing for gateways.
    6 Use IPv6 addressing for gateways.
set ike-version { 1 | 2 } IKE protocol version.
    1 Use IKEv1 protocol.
    2 Use IKEv2 protocol.
set local-gw { ipv4 address } IPv4 address of the local gateway's external interface.
```

```

set local-gw6 { ipv6 address } IPv6 address of the local gateway's external interface.
set remote-gw { ipv4 address } IPv4 address of the remote gateway's external interface.
set remote-gw6 { ipv6 address } IPv6 address of the remote gateway's external interface.
set remotegw-ddns { string } Domain name of remote gateway (eg. name.DDNS.com). size[63]
set keylife { integer } Time to wait in seconds before phase 1 encryption key expires. range[120-172800]
config certificate
  edit { name }
    # The names of up to 4 signed personal certificates.
    set name { string } Certificate name. size[64] - datasource(s): vpn.certificate.local.name
  next
set authmethod { psk | signature } Authentication method.
  psk PSK authentication method.
  signature Signature authentication method.
set authmethod-remote { psk | signature } Authentication method (remote side).
  psk PSK authentication method.
  signature Signature authentication method.
set mode { aggressive | main } The ID protection mode used to establish a secure channel.
  aggressive Aggressive mode.
  main Main mode.
set peertype { option } Accept this peer type.
  any Accept any peer ID.
  one Accept this peer ID.
  dialup Accept peer ID in dialup group.
  peer Accept this peer certificate.
  peergrp Accept this peer certificate group.
set peerid { string } Accept this peer identity. size[255]
set default-gw { ipv4 address } IPv4 address of default route gateway to use for traffic exiting the interface.
set default-gw-priority { integer } Priority for default gateway route. A higher priority number signifies a less preferred route. range[0-4294967295]
set usrgroup { string } User group name for dialup peers. size[35] - datasource(s): user.group.name
set peer { string } Accept this peer certificate. size[35] - datasource(s): user.peer.name
set peergrp { string } Accept this peer certificate group. size[35] - datasource(s): user.peergrp.name
set monitor { string } IPsec interface as backup for primary interface. size[35] - datasource(s): vpn.ipsec.phase1-interface.name
set monitor-hold-down-type { immediate | delay | time } Recovery time method when primary interface re-establishes.
  immediate Fail back immediately after primary recovers.
  delay Number of seconds to delay fail back after primary recovers.
  time Specify a time at which to fail back after primary recovers.
set monitor-hold-down-delay { integer } Time to wait in seconds before recovery once primary re-establishes. range[0-31536000]
set monitor-hold-down-weekday { option } Day of the week to recover once primary re-establishes.
  everyday Every Day.
  sunday Sunday.
  monday Monday.
  tuesday Tuesday.

```

```

    wednesday Wednesday.
    thursday Thursday.
    friday Friday.
    saturday Saturday.
set monitor-hold-down-time { string } Time of day at which to fail back to primary after it re-establishes.
set net-device { enable | disable } Enable/disable kernel device creation for dialup instances.
set tunnel-search { selectors | nexthop } Tunnel search method for when the interface is shared.
    selectors Search for tunnel in selectors.
    nexthop Search for tunnel using nexthop.
set passive-mode { enable | disable } Enable/disable IPsec passive mode for static tunnels.
set exchange-interface-ip { enable | disable } Enable/disable exchange of IPsec interface IP address.
set mode-cfg { disable | enable } Enable/disable configuration method.
set assign-ip { disable | enable } Enable/disable assignment of IP to IPsec interface via configuration method.
set assign-ip-from { range | usrgrp | dhcp | name } Method by which the IP address will be assigned.
    range Assign IP address from locally defined range.
    usrgrp Assign IP address via user group.
    dhcp Assign IP address via DHCP.
    name Assign IP address from firewall address or group.
set ipv4-start-ip { ipv4 address } Start of IPv4 range.
set ipv4-end-ip { ipv4 address } End of IPv4 range.
set ipv4-netmask { ipv4 netmask } IPv4 Netmask.
set dns-mode { manual | auto } DNS server mode.
    manual Manually configure DNS servers.
    auto Use default DNS servers.
set ipv4-dns-server1 { ipv4 address } IPv4 DNS server 1.
set ipv4-dns-server2 { ipv4 address } IPv4 DNS server 2.
set ipv4-dns-server3 { ipv4 address } IPv4 DNS server 3.
set ipv4-wins-server1 { ipv4 address } WINS server 1.
set ipv4-wins-server2 { ipv4 address } WINS server 2.
config ipv4-exclude-range
    edit { id }
        # Configuration Method IPv4 exclude ranges.
        set id { integer } ID. range[0-4294967295]
        set start-ip { ipv4 address } Start of IPv4 exclusive range.
        set end-ip { ipv4 address } End of IPv4 exclusive range.
    next
set ipv4-split-include { string } IPv4 split-include subnets. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set split-include-service { string } Split-include services. size[63] - datasource(s): fire-
wall.service.group.name,firewall.service.custom.name
set ipv4-name { string } IPv4 address name. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set ipv6-start-ip { ipv6 address } Start of IPv6 range.
set ipv6-end-ip { ipv6 address } End of IPv6 range.
set ipv6-prefix { integer } IPv6 prefix. range[1-128]

```

```
set ipv6-dns-server1 { ipv6 address } IPv6 DNS server 1.
set ipv6-dns-server2 { ipv6 address } IPv6 DNS server 2.
set ipv6-dns-server3 { ipv6 address } IPv6 DNS server 3.
config ipv6-exclude-range
  edit { id }
    # Configuration method IPv6 exclude ranges.
    set id { integer } ID. range[0-4294967295]
    set start-ip { ipv6 address } Start of IPv6 exclusive range.
    set end-ip { ipv6 address } End of IPv6 exclusive range.
  next
set ipv6-split-include { string } IPv6 split-include subnets. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set ipv6-name { string } IPv6 address name. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set unity-support { disable | enable } Enable/disable support for Cisco UNITY Configuration Method extensions.
set domain { string } Instruct unity clients about the default DNS domain. size[63]
set banner { string } Message that unity client should display after connecting. size[1024]
set include-local-lan { disable | enable } Enable/disable allow local LAN access on unity clients.
set save-password { disable | enable } Enable/disable saving XAuth username and password on VPN clients.
set client-auto-negotiate { disable | enable } Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.
set client-keep-alive { disable | enable } Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.
config backup-gateway
  edit { address }
    # Instruct unity clients about the backup gateway address(es).
    set address { string } Address of backup gateway. size[64]
  next
set proposal { option } Phase1 proposal.
  des-md5 des-md5
  des-sha1 des-sha1
  des-sha256 des-sha256
  des-sha384 des-sha384
  des-sha512 des-sha512
  3des-md5 3des-md5
  3des-sha1 3des-sha1
  3des-sha256 3des-sha256
  3des-sha384 3des-sha384
  3des-sha512 3des-sha512
  aes128-md5 aes128-md5
  aes128-sha1 aes128-sha1
  aes128-sha256 aes128-sha256
  aes128-sha384 aes128-sha384
  aes128-sha512 aes128-sha512
  aes192-md5 aes192-md5
  aes192-sha1 aes192-sha1
  aes192-sha256 aes192-sha256
```

```

aes192-sha384 aes192-sha384
aes192-sha512 aes192-sha512
aes256-md5 aes256-md5
aes256-sha1 aes256-sha1
aes256-sha256 aes256-sha256
aes256-sha384 aes256-sha384
aes256-sha512 aes256-sha512
aria128-md5 aria128-md5
aria128-sha1 aria128-sha1
aria128-sha256 aria128-sha256
aria128-sha384 aria128-sha384
aria128-sha512 aria128-sha512
aria192-md5 aria192-md5
aria192-sha1 aria192-sha1
aria192-sha256 aria192-sha256
aria192-sha384 aria192-sha384
aria192-sha512 aria192-sha512
aria256-md5 aria256-md5
aria256-sha1 aria256-sha1
aria256-sha256 aria256-sha256
aria256-sha384 aria256-sha384
aria256-sha512 aria256-sha512
seed-md5 seed-md5
seed-sha1 seed-sha1
seed-sha256 seed-sha256
seed-sha384 seed-sha384
seed-sha512 seed-sha512

```

set add-route { disable | enable } Enable/disable control addition of a route to peer destination selector.

set add-gw-route { enable | disable } Enable/disable automatically add a route to the remote gateway.

set psksecret { password_string } Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).

set psksecret-remote { password_string } Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).

set keepalive { integer } NAT-T keep alive interval. range[10-900]

set distance { integer } Distance for routes added by IKE (1 - 255). range[1-255]

set priority { integer } Priority for routes added by IKE (0 - 4294967295). range[0-4294967295]

set localid { string } Local ID. size[63]

set localid-type { option } Local ID type.

auto Select ID type automatically.

fqdn Use fully qualified domain name.

user-fqdn Use user fully qualified domain name.

keyid Use key-id string.

address Use local IP address.

asn1dn Use ASN.1 distinguished name.

```
set auto-negotiate { enable | disable } Enable/disable automatic initiation of IKE SA negotiation.
set negotiate-timeout { integer } IKE SA negotiation timeout in seconds (1 - 300). range[1-300]
set fragmentation { enable | disable } Enable/disable fragment IKE message on re-transmission.
set dpd { disable | on-idle | on-demand } Dead Peer Detection mode.
    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.
set dpd-retrycount { integer } Number of DPD retry attempts. range[0-10]
set dpd-retryinterval { string } DPD retry interval.
set forticlient-enforcement { enable | disable } Enable/disable FortiClient enforcement.
set comments { string } Comment. size[255]
set npu-offload { enable | disable } Enable/disable offloading NPU.
set send-cert-chain { enable | disable } Enable/disable sending certificate chain.
set dhgrp { option } DH group.
    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.
set suite-b { disable | suite-b-gcm-128 | suite-b-gcm-256 } Use Suite-B.
    disable Do not use UI suite.
    suite-b-gcm-128 Use Suite-B-GCM-128.
    suite-b-gcm-256 Use Suite-B-GCM-256.
set eap { enable | disable } Enable/disable IKEv2 EAP authentication.
set eap-identity { use-id-payload | send-request } IKEv2 EAP peer identity type.
    use-id-payload Use IKEv2 IDi payload to resolve peer identity.
    send-request Use EAP identity request to resolve peer identity.
set acct-verify { enable | disable } Enable/disable verification of RADIUS accounting record.
set wizard-type { option } GUI VPN Wizard Type.
    custom Custom VPN configuration.
    dialup-forticlient Dial Up - FortiClient Windows, Mac and Android.
    dialup-ios Dial Up - iPhone / iPad Native IPsec Client.
    dialup-android Dial Up - Android Native IPsec Client.
```



```

    dialup-windows      Dial Up - Windows Native IPsec Client.
    dialup-cisco        Dial Up - Cisco IPsec Client.
    static-fortigate    Site to Site - FortiGate.
    dialup-fortigate    Dial Up - FortiGate.
    static-cisco        Site to Site - Cisco.
    dialup-cisco-fw     Dialup Up - Cisco Firewall.
set xauthtype { option } XAuth type.
    disable Disable.
    client Enable as client.
    pap Enable as server PAP.
    chap Enable as server CHAP.
    auto Enable as server auto.
set reauth { disable | enable } Enable/disable re-authentication upon IKE SA lifetime expiration.
set authusr { string } XAuth user name. size[64]
set authpasswd { password_string } XAuth password (max 35 characters). size[128]
set group-authentication { enable | disable } Enable/disable IKEv2 IDi group authentication.
set group-authentication-secret { password_string } Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by
a leading 0x.)
set authusrgrp { string } Authentication user group. size[35] - datasource(s): user.group.name
set mesh-selector-type { disable | subnet | host } Add selectors containing subsets of the configuration depending on traffic.
    disable Disable.
    subnet Enable addition of matching subnet selector.
    host Enable addition of host to host selector.
set idle-timeout { enable | disable } Enable/disable IPsec tunnel idle timeout.
set idle-timeoutinterval { integer } IPsec tunnel idle timeout in minutes (5 - 43200). range[5-43200]
set ha-sync-esp-seqno { enable | disable } Enable/disable sequence number jump ahead for IPsec HA.
set auto-discovery-sender { enable | disable } Enable/disable sending auto-discovery short-cut messages.
set auto-discovery-receiver { enable | disable } Enable/disable accepting auto-discovery short-cut messages.
set auto-discovery-forwarder { enable | disable } Enable/disable forwarding auto-discovery short-cut messages.
set auto-discovery-psk { enable | disable } Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.
set encapsulation { none | gre | vxlan } Enable/disable GRE/VXLAN encapsulation.
    none No additional encapsulation.
    gre GRE encapsulation.
    vxlan VXLAN encapsulation.
set encapsulation-address { ike | ipv4 | ipv6 } Source for GRE/VXLAN tunnel address.
    ike Use IKE/IPsec gateway addresses.
    ipv4 Specify separate GRE/VXLAN tunnel address.
    ipv6 Specify separate GRE/VXLAN tunnel address.
set encap-local-gw4 { ipv4 address } Local IPv4 address of GRE/VXLAN tunnel.
set encap-local-gw6 { ipv6 address } Local IPv6 address of GRE/VXLAN tunnel.
set encap-remote-gw4 { ipv4 address } Remote IPv4 address of GRE/VXLAN tunnel.
set encap-remote-gw6 { ipv6 address } Remote IPv6 address of GRE/VXLAN tunnel.
set vni { integer } VNI of VXLAN tunnel. range[1-16777215]

```

```

set natTraversal { enable | disable | forced } Enable/disable NAT traversal.
set esn { require | allow | disable } Extended sequence number (ESN) negotiation.
    require Require extended sequence number.
    allow Allow extended sequence number.
    disable Disable extended sequence number.
set fragmentation-mtu { integer } IKE fragmentation MTU (500 - 16000). range[500-16000]
set childless-ike { enable | disable } Enable/disable childless IKEv2 initiation (RFC 6023).
set rekey { enable | disable } Enable/disable phase1 rekey.
set digital-signature-auth { enable | disable } Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).
set signature-hash-alg { sha1 | sha2-256 | sha2-384 | sha2-512 } Digital Signature Authentication hash algorithms.
    sha1 SHA1.
    sha2-256 SHA2-256.
    sha2-384 SHA2-384.
    sha2-512 SHA2-512.
set rsa-signature-format { pkcs1 | pss } Digital Signature Authentication RSA signature format.
    pkcs1 RSASSA PKCS#1 v1.5.
    pss RSASSA Probabilistic Signature Scheme (PSS).
set enforce-unique-id { disable | keep-new | keep-old } Enable/disable peer ID uniqueness check.
    disable Disable peer ID uniqueness enforcement.
    keep-new Enforce peer ID uniqueness, keep new connection if collision found.
    keep-old Enforce peer ID uniqueness, keep old connection if collision found.
next
end

config vpn ipsec phase1
edit { name }
# Configure VPN remote gateway.
set name { string } IPsec remote gateway name. size[35]
set type { static | dynamic | ddns } Remote gateway type.
    static Remote VPN gateway has fixed IP address.
    dynamic Remote VPN gateway has dynamic IP address.
    ddns Remote VPN gateway has dynamic IP address and is a dynamic DNS client.
set interface { string } Local physical, aggregate, or VLAN outgoing interface. size[35] - datasource(s): system.interface.name
set ike-version { 1 | 2 } IKE protocol version.
    1 Use IKEv1 protocol.
    2 Use IKEv2 protocol.
set remote-gw { ipv4 address } Remote VPN gateway.
set local-gw { ipv4 address } Local VPN gateway.
set remotegw-ddns { string } Domain name of remote gateway (eg. name.DDNS.com). size[63]
set keylife { integer } Time to wait in seconds before phase 1 encryption key expires. range[120-172800]
config certificate
edit { name }

```

```

# The names of up to 4 signed personal certificates.
  set name { string } Certificate name. size[64] - datasource(s): vpn.certificate.local.name
next
set authmethod { psk | signature } Authentication method.
  psk PSK authentication method.
  signature Signature authentication method.
set authmethod-remote { psk | signature } Authentication method (remote side).
  psk PSK authentication method.
  signature Signature authentication method.
set mode { aggressive | main } The ID protection mode used to establish a secure channel.
  aggressive Aggressive mode.
  main Main mode.
set peertype { option } Accept this peer type.
  any Accept any peer ID.
  one Accept this peer ID.
  dialup Accept peer ID in dialup group.
  peer Accept this peer certificate.
  peergrp Accept this peer certificate group.
set peerid { string } Accept this peer identity. size[255]
set usrgrp { string } User group name for dialup peers. size[35] - datasource(s): user.group.name
set peer { string } Accept this peer certificate. size[35] - datasource(s): user.peer.name
set peergrp { string } Accept this peer certificate group. size[35] - datasource(s): user.peergrp.name
set autoconfig { disable | client | gateway } Auto-configuration type.
  disable Disable auto-configuration.
  client Enable auto-configuration client.
  gateway Enable auto-configuration gateway.
set mode-cfg { disable | enable } Enable/disable configuration method.
set assign-ip { disable | enable } Enable/disable assignment of IP to IPsec interface via configuration method.
set assign-ip-from { range | usrgrp | dhcp | name } Method by which the IP address will be assigned.
  range Assign IP address from locally defined range.
  usrgrp Assign IP address via user group.
  dhcp Assign IP address via DHCP.
  name Assign IP address from firewall address or group.
set ipv4-start-ip { ipv4 address } Start of IPv4 range.
set ipv4-end-ip { ipv4 address } End of IPv4 range.
set ipv4-netmask { ipv4 netmask } IPv4 Netmask.
set dns-mode { manual | auto } DNS server mode.
  manual Manually configure DNS servers.
  auto Use default DNS servers.
set ipv4-dns-server1 { ipv4 address } IPv4 DNS server 1.
set ipv4-dns-server2 { ipv4 address } IPv4 DNS server 2.
set ipv4-dns-server3 { ipv4 address } IPv4 DNS server 3.
set ipv4-wins-server1 { ipv4 address } WINS server 1.

```

```

set ipv4-wins-server2 { ipv4 address }   WINS server 2.
config ipv4-exclude-range
  edit { id }
  # Configuration Method IPv4 exclude ranges.
  set id { integer }   ID. range[0-4294967295]
  set start-ip { ipv4 address }   Start of IPv4 exclusive range.
  set end-ip { ipv4 address }   End of IPv4 exclusive range.
  next
set ipv4-split-include { string }   IPv4 split-include subnets. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set split-include-service { string }   Split-include services. size[63] - datasource(s): fire-
wall.service.group.name,firewall.service.custom.name
set ipv4-name { string }   IPv4 address name. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set ipv6-start-ip { ipv6 address }   Start of IPv6 range.
set ipv6-end-ip { ipv6 address }   End of IPv6 range.
set ipv6-prefix { integer }   IPv6 prefix. range[1-128]
set ipv6-dns-server1 { ipv6 address }   IPv6 DNS server 1.
set ipv6-dns-server2 { ipv6 address }   IPv6 DNS server 2.
set ipv6-dns-server3 { ipv6 address }   IPv6 DNS server 3.
config ipv6-exclude-range
  edit { id }
  # Configuration method IPv6 exclude ranges.
  set id { integer }   ID. range[0-4294967295]
  set start-ip { ipv6 address }   Start of IPv6 exclusive range.
  set end-ip { ipv6 address }   End of IPv6 exclusive range.
  next
set ipv6-split-include { string }   IPv6 split-include subnets. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set ipv6-name { string }   IPv6 address name. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set unity-support { disable | enable }   Enable/disable support for Cisco UNITY Configuration Method extensions.
set domain { string }   Instruct unity clients about the default DNS domain. size[63]
set banner { string }   Message that unity client should display after connecting. size[1024]
set include-local-lan { disable | enable }   Enable/disable allow local LAN access on unity clients.
set save-password { disable | enable }   Enable/disable saving XAuth username and password on VPN clients.
set client-auto-negotiate { disable | enable }   Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.
set client-keep-alive { disable | enable }   Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.
config backup-gateway
  edit { address }
  # Instruct unity clients about the backup gateway address(es).
  set address { string }   Address of backup gateway. size[64]
  next
set proposal { option }   Phase1 proposal.
  des-md5           des-md5
  des-sha1          des-sha1
  des-sha256        des-sha256

```

```

des-sha384      des-sha384
des-sha512      des-sha512
3des-md5        3des-md5
3des-sha1       3des-sha1
3des-sha256     3des-sha256
3des-sha384     3des-sha384
3des-sha512     3des-sha512
aes128-md5      aes128-md5
aes128-sha1     aes128-sha1
aes128-sha256   aes128-sha256
aes128-sha384   aes128-sha384
aes128-sha512   aes128-sha512
aes192-md5      aes192-md5
aes192-sha1     aes192-sha1
aes192-sha256   aes192-sha256
aes192-sha384   aes192-sha384
aes192-sha512   aes192-sha512
aes256-md5      aes256-md5
aes256-sha1     aes256-sha1
aes256-sha256   aes256-sha256
aes256-sha384   aes256-sha384
aes256-sha512   aes256-sha512
aria128-md5     aria128-md5
aria128-sha1    aria128-sha1
aria128-sha256  aria128-sha256
aria128-sha384  aria128-sha384
aria128-sha512  aria128-sha512
aria192-md5     aria192-md5
aria192-sha1    aria192-sha1
aria192-sha256  aria192-sha256
aria192-sha384  aria192-sha384
aria192-sha512  aria192-sha512
aria256-md5     aria256-md5
aria256-sha1    aria256-sha1
aria256-sha256  aria256-sha256
aria256-sha384  aria256-sha384
aria256-sha512  aria256-sha512
seed-md5        seed-md5
seed-sha1       seed-sha1
seed-sha256     seed-sha256
seed-sha384     seed-sha384
seed-sha512     seed-sha512

```

```
set add-route { disable | enable } Enable/disable control addition of a route to peer destination selector.
```

```
set add-gw-route { enable | disable } Enable/disable automatically add a route to the remote gateway.
set psksecret { password_string } Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).
set psksecret-remote { password_string } Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a
leading 0x).
set keepalive { integer } NAT-T keep alive interval. range[10-900]
set distance { integer } Distance for routes added by IKE (1 - 255). range[1-255]
set priority { integer } Priority for routes added by IKE (0 - 4294967295). range[0-4294967295]
set localid { string } Local ID. size[63]
set localid-type { option } Local ID type.
    auto      Select ID type automatically.
    fqdn      Use fully qualified domain name.
    user-fqdn Use user fully qualified domain name.
    keyid     Use key-id string.
    address   Use local IP address.
    asn1dn    Use ASN.1 distinguished name.
set auto-negotiate { enable | disable } Enable/disable automatic initiation of IKE SA negotiation.
set negotiate-timeout { integer } IKE SA negotiation timeout in seconds (1 - 300). range[1-300]
set fragmentation { enable | disable } Enable/disable fragment IKE message on re-transmission.
set dpd { disable | on-idle | on-demand } Dead Peer Detection mode.
    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.
set dpd-retrycount { integer } Number of DPD retry attempts. range[0-10]
set dpd-retryinterval { string } DPD retry interval.
set forticlient-enforcement { enable | disable } Enable/disable FortiClient enforcement.
set comments { string } Comment. size[255]
set npu-offload { enable | disable } Enable/disable offloading NPU.
set send-cert-chain { enable | disable } Enable/disable sending certificate chain.
set dhgrp { option } DH group.
    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.
set suite-b { disable | suite-b-gcm-128 | suite-b-gcm-256 } Use Suite-B.
    disable Do not use UI suite.
    suite-b-gcm-128 Use Suite-B-GCM-128.
    suite-b-gcm-256 Use Suite-B-GCM-256.
set eap { enable | disable } Enable/disable IKEv2 EAP authentication.
set eap-identity { use-id-payload | send-request } IKEv2 EAP peer identity type.
    use-id-payload Use IKEv2 IDi payload to resolve peer identity.
    send-request Use EAP identity request to resolve peer identity.
set acct-verify { enable | disable } Enable/disable verification of RADIUS accounting record.
set wizard-type { option } GUI VPN Wizard Type.
    custom Custom VPN configuration.
    dialup-forticlient Dial Up - FortiClient Windows, Mac and Android.
    dialup-ios Dial Up - iPhone / iPad Native IPsec Client.
    dialup-android Dial Up - Android Native IPsec Client.
    dialup-windows Dial Up - Windows Native IPsec Client.
    dialup-cisco Dial Up - Cisco IPsec Client.
    static-fortigate Site to Site - FortiGate.
    dialup-fortigate Dial Up - FortiGate.
    static-cisco Site to Site - Cisco.
    dialup-cisco-fw Dialup Up - Cisco Firewall.
set xauthtype { option } XAuth type.
    disable Disable.
    client Enable as client.
    pap Enable as server PAP.
    chap Enable as server CHAP.
    auto Enable as server auto.
set reauth { disable | enable } Enable/disable re-authentication upon IKE SA lifetime expiration.
set authusr { string } XAuth user name. size[64]
set authpasswd { password_string } XAuth password (max 35 characters). size[128]
set group-authentication { enable | disable } Enable/disable IKEv2 IDi group authentication.
set group-authentication-secret { password_string } Password for IKEv2 IDi group authentication. (ASCII string or hexadecimal indicated by
a leading 0x.)
set authsrgrp { string } Authentication user group. size[35] - datasource(s): user.group.name
set mesh-selector-type { disable | subnet | host } Add selectors containing subsets of the configuration depending on traffic.
    disable Disable.
    subnet Enable addition of matching subnet selector.
    host Enable addition of host to host selector.
set idle-timeout { enable | disable } Enable/disable IPsec tunnel idle timeout.
set idle-timeoutinterval { integer } IPsec tunnel idle timeout in minutes (5 - 43200). range[5-43200]
set ha-sync-esp-seqno { enable | disable } Enable/disable sequence number jump ahead for IPsec HA.
set nattraversal { enable | disable | forced } Enable/disable NAT traversal.
set esn { require | allow | disable } Extended sequence number (ESN) negotiation.

```

```

        require Require extended sequence number.
        allow Allow extended sequence number.
        disable Disable extended sequence number.
set fragmentation-mtu { integer } IKE fragmentation MTU (500 - 16000). range[500-16000]
set childless-ike { enable | disable } Enable/disable childless IKEv2 initiation (RFC 6023).
set rekey { enable | disable } Enable/disable phase1 rekey.
set digital-signature-auth { enable | disable } Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).
set signature-hash-alg { sha1 | sha2-256 | sha2-384 | sha2-512 } Digital Signature Authentication hash algorithms.
    sha1 SHA1.
    sha2-256 SHA2-256.
    sha2-384 SHA2-384.
    sha2-512 SHA2-512.
set rsa-signature-format { pkcs1 | pss } Digital Signature Authentication RSA signature format.
    pkcs1 RSASSA PKCS#1 v1.5.
    pss RSASSA Probabilistic Signature Scheme (PSS).
set enforce-unique-id { disable | keep-new | keep-old } Enable/disable peer ID uniqueness check.
    disable Disable peer ID uniqueness enforcement.
    keep-new Enforce peer ID uniqueness, keep new connection if collision found.
    keep-old Enforce peer ID uniqueness, keep old connection if collision found.
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

type {static | dynamic | ddns}

The connection type of the remote gateway:

- Use `static` if the remote VPN peer has a static IP address. Once set, use the `remote-gw` entry to specify the IP address.
- Use `dynamic` if the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE).
- Use `ddns` if the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service. Once set, use the `remotegw-ddns` entry to enter the domain name of the remote VPN peer.

Note: `ddns` is *not* available when `ip-version` is set to 6.

interface <out-interface>

Enter the name of the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.

ip-version {4 | 6}

Enter 4 (by default) for IPv4 or 6 for IPv6 encapsulation for gateways.

ike-version {1 | 2}

Enter 1 (by default) for IKEv1 or 2 for IKEv2 protocol version.

local-gw [sec-addr-ipv4]

An optional secondary IPv4 IP address of the interface selected in the `interface` entry used for the local end of the VPN tunnel.

local-gw6 [sec-addr-ipv6]

Note: This entry is only available when `ip-version` is set to 6. An optional secondary IPv6 IP address of the interface selected in the `interface` entry used for the local end of the VPN tunnel.

remote-gw <addr-ipv4>

Note: This entry is only available when `ip-version` is set to 4 and `type` is set to `static`. The IPv4 IP address of the remote gateway's external interface. Note that this entry is not available when `type` is set to `dynamic`.

remote-gw6 <addr-ipv6>

Note: This entry is only available when `ip-version` is set to 6. The IPv6 IP address of the remote gateway's external interface.

remotegw-ddns <domain-name>

Note: This entry is only available when `ip-version` is set to 4 and `type` is set to `ddns`. The identifier of the remote peer (e.g. an FQDN). This should be used when the remote peer has a static domain name and a dynamic IP address.

keylife <seconds>

The amount of time in seconds before the phase 1 encryption key expires, at which time a new encryption key is generated without service interruption. Set the value between 120-172800 seconds (or two minutes to two days). The default is set to 86400.

certificate <cert-string>

Note: This entry is only available when `authmethod` is set to `signature`. Enter the names of up to four signed personal certificates for the FortiGate unit. The certificates must have already been installed on the FortiGate before entering them here.

authmethod {psk | signature}

Enter your preferred authentication method:

- Use `psk` (by default) to authenticate using a pre-shared key. Once set, use the `psksecret` entry to specify the pre-shared key.
 - Use `signature` to authenticate using a certificate. Once set, use the `certificate` entry to specify the name of the certificate.
-

mode {aggressive | main}

Note: This entry is only available when `ike-version` is set to 1. An ID protection mode that establishes a secure channel.

- Use `aggressive` mode when a remote peer or dialup client has a dynamic IP address. If this is not set, the remote peer will be authenticated using an identifier (local ID). Identifying information is exchanged in the clear.
 - Use `main` mode (by default) when both peers have static IP addresses. Identifying information is hidden.
-

peertype <any | one | peer | peergrp | dialup>

The following `peertype` options are available:

- `any`: Accepts any remote client or peer. Peer IDs are not used for authentication purposes. This is set by default.
- `one`: Authenticates either a remote peer or client that has a dynamic IP address and connects using a unique identifier over a dedicated tunnel, or more than one dialup client that connects through the same tunnel using the same (shared) identifier. Once set, use the `peerid` entry to set the peer ID. If more than one dialup client will be connecting using the same identifier, set `mode` to `aggressive`.

- `peer`: Authenticates one or more certificate holders based on a particular (or shared) certificate. Once set, use the `peer` entry to enter the certificate name. If the remote peer has a dynamic IP address, set `mode` to `aggressive`.
- `peergrp`: Authenticates certificate holders that use unique certificates. In this case, you must create a group of certificate holders for authentication purposes. Once set, use the `peergrp` entry to set the certificate group name. If the remote peer has a dynamic IP address, set `mode` to `aggressive`.
- `dialup`: Authenticates dialup VPN clients that use unique identifiers and/or preshared-keys to connect to the VPN through the same VPN tunnel. In this case, you must create a dialup user group for authentication purposes. Once set, use the `usrgrp` entry to set the user group name. If the dialup clients use unique identifiers and preshared-keys, set `mode` to `aggressive`. If the dialup clients use preshared-keys *only*, set `mode` to `main`.

Availability of these options vary depending on which remote gateway `type` and `authmethod` is used. Below is a table to show which peertypes are available under different circumstances:

type	authmethod	peertype
static	psk	> any
	signature	> any, one, peer, peergrp
dynamic	psk	> any, one, dialup
	signature	> any, one, peer, peergrp
ddns	psk	> any
	signature	> any, one, peer, peergrp

peergrp <peer-group>

Note: This entry is only available when `peertype` is set to `peergrp`. Accepts the specified peer group.

peerid <peer-id>

Note: This entry is only available when `peertype` is set to `one`. Accepts the specified peer identity.

peer <cert-name>

Note: This entry is only available when `type` is configured. Accepts the specified peer certificate.

default-gw <addr-ipv4>

Note: This entry is only available when `type` is set to `dynamic` and `ip-version` is set to 4. The IPv4 address of the default route gateway to use for traffic exiting the interface.

default-gw-priority <priority>

Note: This entry is only available when `type` is set to `dynamic`. The priority for the default gateway router. Set the value between 0-4294967295. Default is set to 0.

usrgrp <group-name>

Note: This entry is only available when `peertype` is set to `dialup`. The user group. You must have already configured a user group on the FortiGate unit before entering the group's name here.

monitor [phase1]

Note: This entry is not available when `type` is set to `dynamic`. An optional IPsec interface that can act as a backup for another (primary) IPsec interface. Enter the name of the primary interface. Once set, use the `monitor-hold-down-type` entry to configure recovery timing (further configured with the `monitor-hold-down-delay`, `monitor-hold-down-weekday`, and `monitor-hold-down-time` entries).

The backup interface is only used when the primary interface is unavailable. For this, `dpd` must be enabled (set to either `on-idle` or `on-timeout`).

Note that a primary interface can only have one backup interface and cannot itself act as a backup for another interface.

monitor-hold-down-type {immediate | delay | time}

Note: This entry (and all other sub-entries) is only available once `monitor` is configured. Controls the recovery time method when the primary interface re-establishes.

- Use `immediate` (by default) to have the primary interface be re-established immediately.
- Use `delay` to configure the number of seconds to wait before recovery once the primary interface is re-established (see the `monitor-hold-down-delay` entry).
- Use `time` to configure the day of the week and/or the time of day to recover once the primary interface is re-established (see the `monitor-hold-down-weekday` and `monitor-hold-down-time` entries).

`monitor-hold-down-delay <seconds>`

Note: This entry is only available when `monitor-hold-down-type` is set to `delay`. Configure the number of seconds to wait before recovery once the primary interface is re-established. Set the value between 0-31536000 (or 0 seconds to 1 year). The default is set to 0.

`monitor-hold-down-weekday <day>`

Note: This entry is only available when `monitor-hold-down-type` is set to `time`. Configure the day of the week to recover once the primary interface is re-established. Set the value to either `everyday`, `sunday` (by default), `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, or `saturday`.

`monitor-hold-down-time <time>`

Note: This entry is only available when `monitor-hold-down-type` is set to `time`. Configure the time of day to recover once the primary interface is re-established. Set the hour and minute values of the day, with a colon to separate the two (between 00:00 and 23:59). The default is set to 00:00 (or midnight).

`mode-cfg {enable | disable}`

Enable IKE Configuration Method so that compatible clients can configure themselves with settings that the FortiGate unit provides. Disable (by default) to prohibit clients from configuring themselves.

`assign-ip {enable | disable}`

Note: This entry is only available when `mode-cfg` is set to `enable`. Enable (by default) or disable the assignment of an IP address to the IPsec interface.

assign-ip-from {range | dhcp}

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The method by which the IP address will be assigned.

- Use `range` (by default) to assign the IP address from a locally defined range.
 - Use `dhcp` to assign the IP address via DHCP.
-

ipv4-start-ip <ipv4-start>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The start of the IPv4 range.

ipv4-end-ip <ipv4-end>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The end of the IPv4 range.

ipv4-netmask <ipv4-netmask>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv4 netmask.

dns-mode {manual | auto}

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The DNS server mode.

- Use `manual` (by default) to manually configure the DNS servers.
 - Use `auto` to use default DNS servers.
-

ipv4-dns-server1 <server1>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify an IPv4 DNS server, of which you may specify up to three (see entries below).

ipv4-dns-server2 <server2>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a second IPv4 DNS server.

ipv4-dns-server3 <server3>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a third IPv4 DNS server.

ipv4-wins-server1 <server1>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Windows Internet Name Service (WINS) is a central mapping of host names to network addresses. Specify a WINS server, of which you may specify up to two (see entry below).

ipv4-wins-server2 <server2>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a second WINS server.

ipv4-exclude-range

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. A configuration method to exclude IPv4 ranges. Edit to create new and specify the exclude-ranges using the `start-ip` and `end-ip` entries.

ipv4-split-include <subnet>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv4 split-include subnets. The addresses must have already been configured on the FortiGate unit before entering their names here.

split-include-service <service>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The split-include services. The services must have already been configured on the FortiGate unit before entering their names here.

ipv4-name <name>

IPv4 address name used when `assign-ip-from` is set to `name`.

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`.

ipv6-start-ip <ipv6-start>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The start of the IPv6 range.

ipv6-end-ip <ipv6-end>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The end of the IPv6 range.

ipv6-prefix <ipv6-prefix>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv6 address' prefix. Enter a value between 1-128. The default is set to 128.

ipv6-dns-server1 <server1>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify an IPv6 DNS server, of which you may specify up to three (see entries below).

ipv6-dns-server2 <server2>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a second IPv6 DNS server.

ipv6-dns-server3 <server3>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Specify a third IPv6 DNS server.

ipv6-exclude-range

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. A configuration method to exclude IPv6 ranges. Edit to create new and specify the exclude-ranges using the `start-ip` and `end-ip` entries.

ipv6-split-include <subnet>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The IPv6 split-include subnets. The addresses must have already been configured on the FortiGate unit before entering their names here.

ipv6-name <name>

IPv6 address name used when `assign-ip-from` is set to `name`.

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`.

unity-support {enable | disable}

Note: This entry is only available when `mode-cfg` is set to `enable`. Enable (by default) or disable support for Cisco Unity configuration method extensions.

domain <domain>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The default DNS domain for Unity clients.

banner <message>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The message that Unity clients should display after connecting.

include-local-lan {enable | disable}

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Enable or disable (by default) allowing local LAN access on Unity clients.

client-auto-negotiate {enable | disable}

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Enable or disable (by default) allowing the VPN client to bring up the tunnel when there is no traffic.

client-keep-alive {enable | disable}

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. Enable or disable (by default) allowing the VPN client to keep the tunnel up when there is no traffic.

backup-gateway <address>

Note: This entry is only available when `type` is set to `dynamic` and `mode-cfg` is set to `enable`. The backup gateway address(es) for Unity clients.

proposal <phase1-proposal>

A minimum of one and maximum of ten encryption-message combinations for the phase 1 proposal, for example `aes128-sha256`. Use a space to separate the combinations. Make sure that the remote peer is configured to use at least one of the proposals defined. **Note:** This entry is *not* available if `suite-b` has been configured. Use any of the following key encryption algorithms:

- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.

- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA and seed algorithms may not be available on some FortiGate models. Combine key encryptions with any one of the following message digests, to check the authenticity of messages during an encrypted session:

- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

add-route {disable | enable}

Note: This entry is only available when `type` is set to `dynamic`. Enable (by default) or disable adding a route to the destination of the peer selector.

exchange-interface-ip {enable | disable}

Enable or disable (by default) the exchange of IPsec interface IP address.

add-gw-route {enable | disable}

Enable to automatically add a route to the remote gateway specified in the `remote-gw` entry. This is disabled by default.

Note: This command is deprecated. Instead, use the `dynamic-gateway {enable | disable}` entry in the `config router static` command.

psksecret <preshared-key>

Note: This entry is only available when `authmethod` is set to `psk`. Enter the pre-shared key. The pre-shared key must be the same on the remote VPN gateway or client and should only be known by network administrators. The key must consist of at least six characters. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

keepalive <seconds>

Note: This entry is only available when `nattraversal` is set to `enable`. Set the NAT traversal keepalive frequency in seconds, a period of time that specifies how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until phase 1 and 2 security associations (SAs) expire. Set the value between 10-900 seconds (or ten seconds to 15 minutes). The default is set to 5.

distance <distance>

Note: This entry is only available when `type` is set to `dynamic`, or when `mode-cfg` is set to `enable`. The distance for routes added by IKE. Set the value between 1-255. Default is set to 15.

priority <priority>

Note: This entry is only available when `type` is set to `dynamic`, or when `mode-cfg` is set to `enable`. The priority for routes added by IKE. Set the value between 0-4294967295. Default is set to 0.

localid <local-id>

Note: If you set a local ID on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup server and specify the identifier as a peer ID on the FortiGate dialup server. The local ID, or unique identifier, that the FortiGate uses as a VPN client for authentication purposes.

localid-type {auto | fqdn | user-fqdn | keyid | address}

Determines the type of local ID to be set:

- `auto`: Selects type automatically.
 - `fqdn`: Uses a Fully Qualified Domain Name (FQDN).
 - `user-fqdn`: Uses a User FQDN.
 - `keyid`: Uses Key Identifier ID.
 - `address`: Uses IP address ID.
-

auto-negotiate {enable | disable}

Enable (by default) to keep attempting IKE SA negotiation even if the link is down. This feature is useful in cases where there are multiple redundant tunnels but you prefer the primary connection if it can be established.

negotiate-timeout <seconds>

The amount of time in seconds that the FortiGate unit will wait for the IKE SA to be negotiated. Set the value between 1-300 seconds (or one second to five minutes). The default is set to 5.

fragmentation {enable | disable}

Note: This entry is only available when `ike-version` is set to 1. Enable (by default) intra-IKE fragmentation support on re-transmission of fragmented packets.

dpd {disable | on-idle | on-demand}

Disable or set Dead Peer Detection (DPD) to either `on-idle` or `on-demand` (by default). DPD detects the status of the connection between VPN peers, cleans up dead connections, and helps establish new VPN tunnels. Note that DPD cannot be used unless both VPN peers support and enable the feature.

- `on-idle`: DPD is triggered when IPsec is idle/inactive.
 - `on-demand`: DPD is triggered when IPsec traffic is sent but no reply is received from the peer.
-

dpd-retrycount <retry-integer>

Note: This entry is only available when `dpd` is set to `enable`. The number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the SA. Set the value between 0-10. The default is set to 3. To avoid false negatives set the retry count to a sufficiently high value for your network.

dpd-retryinterval <seconds> [milliseconds]

Note: This entry is only available when `dpd` is set to `enable`. The amount of time in seconds (and optionally milliseconds) that the local VPN peer waits between sending DPD probes. Use a space to separate the seconds and milliseconds (e.g. for 2.5 seconds, enter `2 500`). Set the value between 0-60

seconds and 0-999 milliseconds.

forticlient-enforcement {enable | disable}

Enable to only permit FortiClient users to connect. Disable (by default) to lift this restriction.

comments [string]

Optional comments.

npu-offload {enable | disable}

Enable (by default) or disable offloading of VPN session to a network processing unit (NPU).

send-cert-chain {enable | disable}

Note: This entry is only available when `authmethod` is set to `signature`. Enable (by default) or disable sending certificate chain.

dhgrp {1 | 2 | 5 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 27 | 28 | 29 | 30}

Apply one or more Diffie-Hellman (DH) group numbers, in order of preference, separated by spaces. DH groups determine the strength of the key used in the key exchange process, with higher group numbers being more secure, but requiring additional time to compute the key. Set the value to any one (or more) of the following: 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, and 30. The default is set to 14 5.

Note that at least one of the group numbers set on the remote peer or client must be identical to one of the selections on the FortiGate unit.

Note: This entry is *not* available if `suite-b` has been configured.

suite-b {disable | suite-b-gcm-128 | suite-b-gcm-256}

Disable (by default) or set Suite B to either `suite-b-gcm-128` or `suite-b-gcm-256`. Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels (see [RFC 6379](#), [Suite B Cryptographic Suites for IPsec](#)).

- Suite-B-GCM-128 applies Advanced Encryption Standard (AES) encryption with 128-bit keys and 16-octet integrity check value (OCV) in Galois/Counter Mode (GCM), a mode of operation for symmetric key cryptographic block ciphers. Key establishment uses DH group 19.
- Suite-B-GCM-256 applies AES encryption with 256-bit keys and 16-octet ICV in GCM. Key establishment uses DH group 20.

eap {enable | disable}

Note: This entry is only available when `ike-version` is set to 2. Enable or disable (by default) IKEv2 Extensible Authentication Protocol (EAP) authentication.

eap-identity {use-id-payload | send-request}

Note: This entry is only available when `eap` is set to `enable`. The IKEv2 EAP peer identity type.

- `use-id-payload` uses IKEv2 identity payload to resolve peer identity. This is set by default.
- `send-request` uses EAP identity request to resolve peer identity.

acct-verify {enable | disable}

Note: This entry is only available when `eap` is set to `enable`. Enable or disable (by default) the verification of RADIUS accounting record.

wizard-type <wizard-type>

Set to one of the following GUI VPN Wizard template types:

- `custom`: Custom VPN configuration.
- `dialup-forticlient`: Dialup for FortiClient Windows, Mac, and Android.
- `dialup-ios`: Dialup for iPhone and/or iPad Native IPsec Client.
- `dialup-android`: Dialup for Android Native IPsec Client.
- `dialup-windows`: Dialup for Windows Native IPsec Client.
- `dialup-cisco`: Dialup for Cisco IPsec Client.
- `static-fortigate`: Site to Site for FortiGate.
- `dialup-fortigate`: Dialup for FortiGate.

- `static-cisco`: Site to Site for Cisco.
- `dialup-cisco-fw`: Dialup for Cisco Firewall.

xauthtype [disable | client | pap | chap | auto]

Note: This entry is only available when `ike-version` is set to 1. Optionally configure XAuth (eXtended Authentication). XAuth provides the mechanism for requesting individual authentication information from the user, while a local user database or an external authentication server (such as a RADIUS server) provides a method for storing the authentication information centrally in the local network. This command is disabled by default. Use `pap`, `chap`, or `auto` to configure the FortiGate unit as an XAuth server. Note that these options are only available when `type` is set to `dynamic`.

- `disable`: Disables XAuth.
- `client`: Enable to configure the FortiGate as an XAuth client. Once set, use the `authusr` and `authpasswd` entries to add the XAuth user name and password (see entries below).
- `pap`: Password Authentication Protocol (PAP). Once set, use the `authusrgrp` field to specify the user group containing members that will be authenticated using XAuth.
- `chap`: Challenge Handshake Authentication Protocol (CHAP). Once set, use the `authusrgrp` field to specify the user group containing members that will be authenticated using XAuth.
- `auto`: Enable as server auto. Once set, use the `authusrgrp` field to specify the user group containing members that will be authenticated using XAuth.

reauth {enable | disable}

Note: This entry is only available when `ike-version` is set to 2. Enable or disable (by default) re-authentication upon IKE SA lifetime expiration.

authusrgrp <group-name>

Note: This entry is only available when `eap` is set to `enable`. The authentication user group. You must have already configured a user group on the FortiGate unit before entering the group's name here.

authusr <name>

Note: This entry is only available when `xauthtype` has been configured. Enter the XAuth user name.

authpasswd <password>

Note: This entry is only available when `xauthtype` has been configured. Enter the XAuth user's password (maximum of 35 characters).

mesh-selector-type {disable | subnet | host}

Note: This entry is only available when `ike-version` is set to 1. Disable (by default) or set dynamic mesh selectors for IKEv1 VPNs to either `subnet` or `host`. Note that dynamic selectors are *not* saved to the configuration and will be removed when tunnels are flushed.

- Use `subnet` to install selector for the address group that matches traffic packets.
 - Use `host` to install selector for the source and destination IP addresses of traffic packets.
-

idle-timeout {enable | disable}

Enable or disable (by default) IPsec tunnel to timeout when idle. Once enabled, use the `idle-timeoutinterval` entry to set the period of time the VPN will wait before timing out (see entry below).

idle-timeoutinterval <minutes>

Note: This entry is only available when `idle-timeout` is set to `enable`. Enter the IPsec tunnel idle timeout in minutes. Set the value between 10-43200 (or ten minutes to 30 days). The default is set to 15.

ha-sync-esp-seqno {enable | disable}

Enable (by default) or disable the Extended Sequence Number (ESP) jump ahead for IPsec HA. Enabling this feature helps to synchronize the IPsec SA replay counters between newly active HA cluster members and the peer (see [RFC 6311, Protocol Support for High Availability of IKEv2/IPsec](#)).

auto-discovery-sender {enable | disable}

Auto Discovery VPN (ADVPN) allows a shortcut to be created between two VPN peers, establishing dynamic on-demand tunnels between each other to avoid routing through the topology's hub device. Enable or disable (by default) sending auto-discovery short-cut messages.

auto-discovery-receiver {enable | disable}

Enable or disable (by default) accepting auto-discovery short-cut messages (see the `auto-discovery-sender` entry above about Auto Discovery).

auto-discovery-forwarder {enable | disable}

Enable or disable (by default) forwarding auto-discovery short-cut messages (see the `auto-discovery-sender` entry above about Auto Discovery).

auto-discovery-psk {enable | disable}

Note: This entry is only available when `authmethod` is set to `signature` and `auto-discovery-sender` is set to `enable`. Enable or disable (by default) the use of pre-shared keys for the authentication of auto-discovery tunnels.

encapsulation {none | gre | vxlan}

Note: This entry is *not* available when `type` is set to `dynamic`. Disable (by default; `none`) or set `encapsulation` to either `gre` or `vxlan`. Both GRE and VXLAN segmentation scale well together as they allow overlapping subnets and IP ranges. VXLAN is encapsulated in UDP frames, resulting in efficiently distributed traffic. Once set, use the `.` Both GRE and VXLAN segmentation scale well together as they allow overlapping subnets and IP ranges. VXLAN is encapsulated in UDP frames, resulting in efficiently distributed traffic. Once set, use the `encapsulation-address` entry to configure the source for the GRE or VXLAN tunnel address.

encapsulation-address {ike | ipv4 | ipv6}

Note: This entry is only available when `encapsulation` is set to either `gre` or `vxlan`. Select the source for the GRE or VXLAN tunnel address.

- Use `ike` (by default) to use IKE/IPsec gateway addresses.
 - Use `ipv4` to specify separate IPv4 GRE/VXLAN tunnel addresses (see `encap` entries below).
 - Use `ipv6` to specify separate IPv6 GRE/VXLAN tunnel addresses (see `encap` entries below).
-

encap-local-gw4 <addr-ipv4>

Note: This entry is only available when `encapsulation-address` is set to `ipv4`. The local IPv4 address of the GRE/VXLAN tunnel.

encap-remote-gw4 <addr-ipv4>

Note: This entry is only available when `encapsulation-address` is set to `ipv4`. The remote IPv4 address of the GRE/VXLAN tunnel.

encap-local-gw6 <addr-ipv6>

Note: This entry is only available when `encapsulation-address` is set to `ipv6`. The local IPv6 address of the GRE/VXLAN tunnel.

encap-remote-gw6 <addr-ipv6>

Note: This entry is only available when `encapsulation-address` is set to `ipv6`. The remote IPv6 address of the GRE/VXLAN tunnel.

nattraversal {enable | disable}

Enable (by default) or disable NAT traversal. This should be enabled if you expect the IPsec VPN traffic to go through a gateway that performs NAT. If not NAT device is detected, enabling NAT traversal has no effect. Once enabled, use the `keepalive` entry to set the NAT traversal keepalive frequency. Note that both ends of the VPN must have the same NAT traversal settings.

fragmentation-mtu <frag-integer>

Note: This entry is only available when `ike-version` is set to 2. The IKE fragmentation maximum transmission unit (MTU). Set the value between 500-16000. The default is set to 1200.

childless-ike {enable | disable}

Note: This entry is only available when `ike-version` is set to 2. Enable or disable the childless IKEv2 initiation (see [RFC 6023, A Childless of the Internet Key Exchange Version 2 \(IKEv2\) Security Association \(SA\)](#)).

group-authentication {enable | disable}

Enable or disable (by default) IKEv2 IDi group authentication.

The IDi information is extracted from the IKEv2 AUTH exchange and is sent to a RADIUS server, along with a fixed password, to perform an additional group authentication step prior to tunnel establishment.

The RADIUS server may return framed-IP-address, framed-ip-netmask, and dns-server attributes, which are then applied to the tunnel.

Note: This entry is only available when `ike-version` is set to 2, `type` is set to `dynamic`, and `mode-cfg` is set to `enable`.

group-authentication-secret <password>

Password for IKEv2 IDi group authentication (ASCII string or hexadecimal indicated by a leading 0x).

Note: This entry is only available when `group-authentication` is set to `enable`.

vpn ipsec {phase2-interface | phase2}

Use `phase2-interface` to add or edit a phase 2 configuration on a route-based (interface mode) IPsec tunnel. This command is only available in NAT/Route mode. You can also use `phase2` to add or edit IPsec tunnel-mode phase 2 configurations to create and maintain IPsec VPN tunnels with a remote VPN gateway or client peer. **Note:** The following entries are *not* available under the `phase2` command:

- `auto-discovery-sender`
- `auto-discovery-forwarder`

```
config vpn ipsec phase2-interface
edit { name }
# Configure VPN autokey tunnel.
set name { string } IPsec tunnel name. size[35]
set phase1name { string } Phase 1 determines the options required for phase 2. size[15] - datasource(s): vpn.ipsec.phase1-interface.name
set dhcp-ipsec { enable | disable } Enable/disable DHCP-IPsec.
set proposal { option } Phase2 proposal.
    null-md5      null-md5
    null-sha1     null-sha1
    null-sha256   null-sha256
    null-sha384   null-sha384
    null-sha512   null-sha512
    des-null      des-null
    des-md5       des-md5
    des-sha1      des-sha1
    des-sha256    des-sha256
    des-sha384    des-sha384
    des-sha512    des-sha512
    3des-null     3des-null
    3des-md5      3des-md5
    3des-sha1     3des-sha1
    3des-sha256   3des-sha256
    3des-sha384   3des-sha384
    3des-sha512   3des-sha512
    aes128-null   aes128-null
    aes128-md5    aes128-md5
    aes128-sha1   aes128-sha1
    aes128-sha256 aes128-sha256
    aes128-sha384 aes128-sha384
```

```

aes128-sha512 aes128-sha512
aes128gcm aes128gcm
aes192-null aes192-null
aes192-md5 aes192-md5
aes192-sha1 aes192-sha1
aes192-sha256 aes192-sha256
aes192-sha384 aes192-sha384
aes192-sha512 aes192-sha512
aes256-null aes256-null
aes256-md5 aes256-md5
aes256-sha1 aes256-sha1
aes256-sha256 aes256-sha256
aes256-sha384 aes256-sha384
aes256-sha512 aes256-sha512
aes256gcm aes256gcm
aria128-null aria128-null
aria128-md5 aria128-md5
aria128-sha1 aria128-sha1
aria128-sha256 aria128-sha256
aria128-sha384 aria128-sha384
aria128-sha512 aria128-sha512
aria192-null aria192-null
aria192-md5 aria192-md5
aria192-sha1 aria192-sha1
aria192-sha256 aria192-sha256
aria192-sha384 aria192-sha384
aria192-sha512 aria192-sha512
aria256-null aria256-null
aria256-md5 aria256-md5
aria256-sha1 aria256-sha1
aria256-sha256 aria256-sha256
aria256-sha384 aria256-sha384
aria256-sha512 aria256-sha512
seed-null seed-null
seed-md5 seed-md5
seed-sha1 seed-sha1
seed-sha256 seed-sha256
seed-sha384 seed-sha384
seed-sha512 seed-sha512

```

```
set pfs { enable | disable } Enable/disable PFS feature.
```

```
set dhgrp { option } Phase2 DH group.
```

- 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.

set replay { enable | disable }  Enable/disable replay detection.
set keepalive { enable | disable }  Enable/disable keep alive.
set auto-negotiate { enable | disable }  Enable/disable IPsec SA auto-negotiation.
set add-route { phase1 | enable | disable }  Enable/disable automatic route addition.
set auto-discovery-sender { phase1 | enable | disable }  Enable/disable sending short-cut messages.
set auto-discovery-forwarder { phase1 | enable | disable }  Enable/disable forwarding short-cut messages.
set keylifeseconds { integer }  Phase2 key life in time in seconds (120 - 172800). range[120-172800]
set keylifekbs { integer }  Phase2 key life in number of bytes of traffic (5120 - 4294967295). range[5120-4294967295]
set keylife-type { seconds | kbs | both }  Keylife type.
    seconds  Key life in seconds.
    kbs      Key life in kilobytes.
    both     Key life both.

set single-source { enable | disable }  Enable/disable single source IP restriction.
set route-overlap { use-old | use-new | allow }  Action for overlapping routes.
    use-old  Use the old route and do not add the new route.
    use-new  Delete the old route and add the new route.
    allow    Allow overlapping routes.

set encapsulation { tunnel-mode | transport-mode }  ESP encapsulation mode.
    tunnel-mode  Use tunnel mode encapsulation.
    transport-mode  Use transport mode encapsulation.

set l2tp { enable | disable }  Enable/disable L2TP over IPsec.
set comments { string }  Comment. size[255]
set protocol { integer }  Quick mode protocol selector (1 - 255 or 0 for all). range[0-255]
set src-name { string }  Local proxy ID name. size[63] - datasource(s): firewall.address.name, firewall.addrgrp.name
set src-name6 { string }  Local proxy ID name. size[63] - datasource(s): firewall.address6.name, firewall.addrgrp6.name
set src-addr-type { option }  Local proxy ID type.
    subnet  IPv4 subnet.
    range   IPv4 range.
    ip      IPv4 IP.
    name    IPv4 firewall address or group name.
```

```

        subnet6 IPv6 subnet.
        range6 IPv6 range.
        ip6 IPv6 IP.
        name6 IPv6 firewall address or group name.
set src-start-ip { ipv4 address any } Local proxy ID start.
set src-start-ip6 { ipv6 address } Local proxy ID IPv6 start.
set src-end-ip { ipv4 address any } Local proxy ID end.
set src-end-ip6 { ipv6 address } Local proxy ID IPv6 end.
set src-subnet { ipv4 classnet any } Local proxy ID subnet.
set src-subnet6 { ipv6 prefix } Local proxy ID IPv6 subnet.
set src-port { integer } Quick mode source port (1 - 65535 or 0 for all). range[0-65535]
set dst-name { string } Remote proxy ID name. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set dst-name6 { string } Remote proxy ID name. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set dst-addr-type { option } Remote proxy ID type.
        subnet IPv4 subnet.
        range IPv4 range.
        ip IPv4 IP.
        name IPv4 firewall address or group name.
        subnet6 IPv6 subnet.
        range6 IPv6 range.
        ip6 IPv6 IP.
        name6 IPv6 firewall address or group name.
set dst-start-ip { ipv4 address any } Remote proxy ID IPv4 start.
set dst-start-ip6 { ipv6 address } Remote proxy ID IPv6 start.
set dst-end-ip { ipv4 address any } Remote proxy ID IPv4 end.
set dst-end-ip6 { ipv6 address } Remote proxy ID IPv6 end.
set dst-subnet { ipv4 classnet any } Remote proxy ID IPv4 subnet.
set dst-subnet6 { ipv6 prefix } Remote proxy ID IPv6 subnet.
set dst-port { integer } Quick mode destination port (1 - 65535 or 0 for all). range[0-65535]
next
end

config vpn ipsec phase2
edit { name }
# Configure VPN autokey tunnel.
set name { string } IPsec tunnel name. size[35]
set phase1name { string } Phase 1 determines the options required for phase 2. size[35] - datasource(s): vpn.ipsec.phase1.name
set dhcp-ipsec { enable | disable } Enable/disable DHCP-IPsec.
set use-natip { enable | disable } Enable to use the FortiGate public IP as the source selector when outbound NAT is used.
set selector-match { exact | subset | auto } Match type to use when comparing selectors.
        exact Match selectors exactly.
        subset Match selectors by subset.

```



```
    auto      Use subset or exact match depending on selector address type.
set proposal { option } Phase2 proposal.
    null-md5      null-md5
    null-sha1     null-sha1
    null-sha256  null-sha256
    null-sha384  null-sha384
    null-sha512  null-sha512
    des-null     des-null
    des-md5      des-md5
    des-sha1     des-sha1
    des-sha256  des-sha256
    des-sha384  des-sha384
    des-sha512  des-sha512
    3des-null    3des-null
    3des-md5     3des-md5
    3des-sha1    3des-sha1
    3des-sha256  3des-sha256
    3des-sha384  3des-sha384
    3des-sha512  3des-sha512
    aes128-null  aes128-null
    aes128-md5   aes128-md5
    aes128-sha1  aes128-sha1
    aes128-sha256 aes128-sha256
    aes128-sha384 aes128-sha384
    aes128-sha512 aes128-sha512
    aes128gcm    aes128gcm
    aes192-null  aes192-null
    aes192-md5   aes192-md5
    aes192-sha1  aes192-sha1
    aes192-sha256 aes192-sha256
    aes192-sha384 aes192-sha384
    aes192-sha512 aes192-sha512
    aes256-null  aes256-null
    aes256-md5   aes256-md5
    aes256-sha1  aes256-sha1
    aes256-sha256 aes256-sha256
    aes256-sha384 aes256-sha384
    aes256-sha512 aes256-sha512
    aes256gcm    aes256gcm
    arial28-null arial28-null
    arial28-md5  arial28-md5
    arial28-sha1 arial28-sha1
    arial28-sha256 arial28-sha256
```

```

    arial28-sha384 arial28-sha384
    arial28-sha512 arial28-sha512
    arial92-null arial92-null
    arial92-md5 arial92-md5
    arial92-sha1 arial92-sha1
    arial92-sha256 arial92-sha256
    arial92-sha384 arial92-sha384
    arial92-sha512 arial92-sha512
    aria256-null aria256-null
    aria256-md5 aria256-md5
    aria256-sha1 aria256-sha1
    aria256-sha256 aria256-sha256
    aria256-sha384 aria256-sha384
    aria256-sha512 aria256-sha512
    seed-null seed-null
    seed-md5 seed-md5
    seed-sha1 seed-sha1
    seed-sha256 seed-sha256
    seed-sha384 seed-sha384
    seed-sha512 seed-sha512
set pfs { enable | disable } Enable/disable PFS feature.
set dhgrp { option } Phase2 DH group.
    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.
set replay { enable | disable } Enable/disable replay detection.
set keepalive { enable | disable } Enable/disable keep alive.
set auto-negotiate { enable | disable } Enable/disable IPsec SA auto-negotiation.
set add-route { phase1 | enable | disable } Enable/disable automatic route addition.
set keylifeseconds { integer } Phase2 key life in time in seconds (120 - 172800). range[120-172800]
set keylifekbs { integer } Phase2 key life in number of bytes of traffic (5120 - 4294967295). range[5120-4294967295]

```

```
set keylife-type { seconds | kbs | both }    Keylife type.
    seconds    Key life in seconds.
    kbs        Key life in kilobytes.
    both       Key life both.
set single-source { enable | disable }    Enable/disable single source IP restriction.
set route-overlap { use-old | use-new | allow }    Action for overlapping routes.
    use-old    Use the old route and do not add the new route.
    use-new    Delete the old route and add the new route.
    allow      Allow overlapping routes.
set encapsulation { tunnel-mode | transport-mode }    ESP encapsulation mode.
    tunnel-mode    Use tunnel mode encapsulation.
    transport-mode Use transport mode encapsulation.
set l2tp { enable | disable }    Enable/disable L2TP over IPsec.
set comments { string }    Comment. size[255]
set protocol { integer }    Quick mode protocol selector (1 - 255 or 0 for all). range[0-255]
set src-name { string }    Local proxy ID name. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set src-name6 { string }    Local proxy ID name. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set src-addr-type { subnet | range | ip | name }    Local proxy ID type.
    subnet    IPv4 subnet.
    range     IPv4 range.
    ip        IPv4 IP.
    name      IPv4 firewall address or group name.
set src-start-ip { ipv4 address any }    Local proxy ID start.
set src-start-ip6 { ipv6 address }    Local proxy ID IPv6 start.
set src-end-ip { ipv4 address any }    Local proxy ID end.
set src-end-ip6 { ipv6 address }    Local proxy ID IPv6 end.
set src-subnet { ipv4 classnet any }    Local proxy ID subnet.
set src-subnet6 { ipv6 prefix }    Local proxy ID IPv6 subnet.
set src-port { integer }    Quick mode source port (1 - 65535 or 0 for all). range[0-65535]
set dst-name { string }    Remote proxy ID name. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
set dst-name6 { string }    Remote proxy ID name. size[63] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
set dst-addr-type { subnet | range | ip | name }    Remote proxy ID type.
    subnet    IPv4 subnet.
    range     IPv4 range.
    ip        IPv4 IP.
    name      IPv4 firewall address or group name.
set dst-start-ip { ipv4 address any }    Remote proxy ID IPv4 start.
set dst-start-ip6 { ipv6 address }    Remote proxy ID IPv6 start.
set dst-end-ip { ipv4 address any }    Remote proxy ID IPv4 end.
set dst-end-ip6 { ipv6 address }    Remote proxy ID IPv6 end.
set dst-subnet { ipv4 classnet any }    Remote proxy ID IPv4 subnet.
set dst-subnet6 { ipv6 prefix }    Remote proxy ID IPv6 subnet.
set dst-port { integer }    Quick mode destination port (1 - 65535 or 0 for all). range[0-65535]
```

```
    next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

phase1name <gateway_name>

The name of the phase 1 gateway configuration, most commonly created using the IPsec Wizard. You must have already added the phase 1 gateway definition to the FortiGate configuration before it can be added here.

dhcp-ipsec {enable | disable}

Enable or disable (by default) DHCP-IPsec.

use-natip {enable | disable}

Enable (by default) or disable the FortiGate to use its public interface IP address as the source selector when outbound NAT is used.

selector-match {exact | subset | auto}

The match-type to use when comparing selectors.

- Use `exact` to match selectors exactly.
- Use `subset` to match selectors by subset.
- Use `auto` (by default) to use subset or exact match depending on the selector address type.

proposal <phase2_proposal>

A minimum of one and maximum of ten encryption-message combinations for the phase 2 proposal, for example `aes128-sha256`. Use a space to separate the combinations. Make sure that the remote peer is configured to use at least one of the proposals defined. Use any of the following key encryption algorithms:

- `des`: Digital Encryption Standard (DES), a 64-bit block algorithm that uses a 56-bit key.
- `3des`: Triple-DES, in which plain text is encrypted three times by three keys.
- `aes128`: A 128-bit block algorithm that uses a 128-bit key.
- `aes192`: A 128-bit block algorithm that uses a 192-bit key.
- `aes256`: A 128-bit block algorithm that uses a 256-bit key.
- `aria128`: A 128-bit Korean block algorithm that uses a 128-bit key.
- `aris192`: A 128-bit Korean block algorithm that uses a 192-bit key.
- `aria256`: A 128-bit Korean block algorithm that uses a 256-bit key.
- `seed`: A 128-bit Korean block algorithm that uses a 128-bit key.

The ARIA and seed algorithms may not be available on some FortiGate models. Combine key encryptions with any one of the following message digests, to check the authenticity of messages during an encrypted session: The ARIA and seed algorithms may not be available on some FortiGate models. Combine key encryptions with any one of the following message digests, to check the authenticity of messages during an encrypted session:

- `md5`: Message Digest (MD) 5, the hash algorithm developed by RSA Data Security.
- `sha1`: Secure Hash Algorithm (SHA) 1 producing a 160-bit message digest.
- `sha256`: SHA 2 producing a 256-bit message digest.
- `sha384`: SHA 2 producing a 384-bit message digest.
- `sha512`: SHA 2 producing a 512-bit message digest.

pfs {enable | disable}

Enable (by default) or disable perfect forward secrecy (PFS). When enabled, encrypted communications and sessions recorded in the past cannot be retrieved and decrypted, should long-term secret keys or passwords be compromised in the future.

dhgrp {1 2 5 14 15 16 17 18 19 20 21 27 28 29 30}

Apply one or more Diffie-Hellman (DH) group numbers, in order of preference, separated by spaces. DH groups determine the strength of the key used in the key exchange process, with higher group numbers being more secure, but requiring additional time to compute the key. Set the value to any one (or more) of the following: 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, and 30. The default is set to 14 5.

Note that at least one of the group numbers set on the remote peer or client must be identical to one of the selections on the FortiGate unit.

replay {enable | disable}

Enable (by default) or disable replay attack detection. When enabled, replay detection discards received packets if they contain a sequence number before the current window, in which case they are seen as being too old, or if they contain a sequence number which has already been received by the FortiGate unit.

keepalive {enable | disable}

Enable or disable (by default) the NAT traversal keepalive frequency, a period of time that specifies how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until phase 1 and 2 security associations (SAs) expire.

add-route {phase1 | enable | disable}

Enable, disable, or set to `phase1` (by default) to add route according to phase add-route settings.

auto-negotiate {enable | disable}

Enable to keep attempting IKE SA negotiation even if the link is down. This feature is useful in cases where there are multiple redundant tunnels but you prefer the primary connection if it can be established. This is set to `enable` to keep attempting IKE SA negotiation even if the link is down. This feature is useful in cases where there are multiple redundant tunnels but you prefer the primary connection if it can be established. This is set to `disable` by default.

auto-discovery-sender {phase1 | enable | disable}

Auto Discovery VPN (ADVPN) allows a shortcut to be created between two VPN peers, establishing dynamic on-demand tunnels between each other to avoid routing through the topology's hub device. Enable or disable sending auto-discovery short-cut messages, or set to `phase1` (by default) to forward short-cut messages according to the `phase1 auto-discovery-sender` setting.

auto-discovery-forwarder {phase1 | enable | disable}

Enable or disable forwarding auto-discovery short-cut messages (see the `auto-discovery-sender` entry above about Auto Discovery), or set to `phase1` (by default) to forward short-cut messages according to the `phase1 auto-discovery-forwarder` setting.

keylifeseconds <seconds>

The amount of time in seconds before the phase 2 encryption key expires, at which time a new encryption key is generated without service interruption. Set the value between 120-172800 seconds (or two minutes to two days). The default is set to 86400.

keylifekbs <bytes>

The number of bytes before the phase 2 encryption key expires, at which point a new encryption key is generated without service interruption. Set the value between 5120-4294967295 bytes (or 5.12KB to 4.29GB). The default is set to 5120. While it is possible to set the value to lower than the default, it is not recommended.

keylife-type {seconds | kbs | both}

The phase 2 encryption key expiration type, used to determine when/how a new encryption key is generated without service interruption. Use `seconds` to then set the key life in seconds, or `kbs` to set the key life in kilobytes (see `keylife` entries above). Use `both` to be able to set both parameters.

single-source {enable | disable}

Note: This entry is *not* available when `l2tp` is set to `enable`. Enable or disable (by default) single source IP restrictions.

- `enable` only accepts single source IPs.
 - `disable` accepts source IP range.
-

route-overlap {use-old | use-new | allow}

Note: This entry is *not* available when `l2tp` is set to `enable`. The action taken for overlapping routes.

- `use-old` uses the old route and does not add the new route.
 - `use-new` deletes the old route and adds the new route.
 - `allow` permits overlapping routes.
-

encapsulation {tunnel-mode | transport-mode}

The Encapsulating Security Payload (ESP) encapsulation mode.

- Use `tunnel-mode` to protect the entire inner IP packet, including the inner IP header.
- Use `transport-mode` to insert ESP after the IP header and before a next layer protocol, e.g. TCP, UDP, ICMP, and so on.

l2tp {enable | disable}

Enable or disable (by default) L2TP over IPsec.

comments [string]

Optional comments.

protocol <integer>

The quick mode protocol selector. Set the value between 1-255, or 0 (by default) for all.

src-addr-type {subnet | range | ip | name | subnet6 | range6 | ip6 | name6}

Note: This entry is only available when `encapsulation` is set to `tunnel-mode`. The local proxy ID type. The default is set to `subnet`. Use `name` to set type to firewall address or group name. Entries with 6 appended to them allow you to set IPv6 options; the other entries allow you to set IPv4 options (see entries below).

{src-subnet | src-subnet6} <ip_netmask>

Note: This entry is only available when `encapsulation` is set to `tunnel-mode`. The entry with 6 appended is only available when `src-addr-type` is set to `subnet6`. The local proxy ID subnet, either IPv4 or IPv6.

src-port <integer>

The quick mode source port. Set the value between 1-65535, or 0 (by default) for all.

{src-start-ip | src-start-ip6} <start_ip>

Note: This entry is only available when `src-addr-type` is set to either `range/range6` or `ip/ip6`. The local proxy ID start, either IPv4 or IPv6.

{src-end-ip | src-end-ip6} <end_ip>

Note: This entry is only available when `src-addr-type` is set to `range`. The local proxy ID end, either IPv4 or IPv6.

{src-name | src-name6} <name>

Note: This entry is only available when `src-addr-type` is set to `name`. The local proxy ID name, either IPv4 or IPv6.

dst-addr-type {subnet | range | ip | name | subnet6 | range6 | ip6 | name6}

Note: This entry is only available when `encapsulation` is set to `tunnel-mode`. The remote proxy ID type. The default is set to `subnet`. Use `name` to set type to firewall address or group name. Entries with `6` appended to them allow you to set IPv6 options; the other entries allow you to set IPv4 options (see entries below).

{dst-subnet | dst-subnet6} <ip_netmask>

Note: This entry is only available when `encapsulation` is set to `tunnel-mode`. The entry with `6` appended is only available when `dst-addr-type` is set to `subnet6`. The remote proxy ID subnet, either IPv4 or IPv6.

dst-port <integer>

The quick mode destination port. Set the value between 1-65535, or 0 (by default) for all.

{dst-start-ip | dst-start-ip6} <start_ip>

Note: This entry is only available when `dst-addr-type` is set to either `range` or `ip`. The remote proxy ID start, either IPv4 or IPv6.

{dst-end-ip | dst-end-ip6} <end_ip>

Note: This entry is only available when `dst-addr-type` is set to `range`. The remote proxy ID end, either IPv4 or IPv6.

{dst-name | dst-name6} <name>

Note: This entry is only available when `dst-addr-type` is set to `name`. The remote proxy ID name, either IPv4 or IPv6.

vpn l2tp

Introduction.

```
config vpn l2tp
  set eip { ipv4 address }   End IP.
  set sip { ipv4 address }   Start IP.
  set status { enable | disable }  Enable/disable FortiGate as a L2TP gateway.
  set usrgrp { string }      User group. size[35] - datasource(s): user.group.name
  set enforce-ipsec { enable | disable }  Enable/disable IPsec enforcement.
end
```

vpn pptp

Introduction.

```
config vpn pptp
  set status { enable | disable }  Enable/disable FortiGate as a PPTP gateway.
  set ip-mode { range | usrgrp }  IP assignment mode for PPTP client.
    range  PPTP client IP from manual config (range from sip to eip).
    usrgrp PPTP client IP from user-group defined server.
  set eip { ipv4 address }  End IP.
  set sip { ipv4 address }  Start IP.
  set local-ip { ipv4 address }  Local IP to be used for peer's remote IP.
  set usrgrp { string }  User group. size[35] - datasource(s): user.group.name
end
```

vpn ssl settings

Use this command to configure basic SSL VPN settings including idle-timeout values and SSL encryption preferences. If required, you can also enable the use of digital certificates for authenticating remote clients, and specify the IP address of any DNS and/or WINS server that resides on the private network behind the FortiGate unit.

Note: SSL VPNs and their commands are only configurable in NAT/Route mode.

```
config vpn ssl settings
  set reqclientcert { enable | disable }  Enable to require client certificates for all SSL-VPN users.
  set sslv3 { enable | disable }  Enable/disable SSLv3.
  set tlsv1-0 { enable | disable }  Enable/disable TLSv1.0.
  set tlsv1-1 { enable | disable }  Enable/disable TLSv1.1.
  set tlsv1-2 { enable | disable }  Enable/disable TLSv1.2.
  set banned-cipher { option }  Select one or more cipher technologies that cannot be used in SSL-VPN negotiations.
    RSA      Ban the use of cipher suites using RSA key.
    DH       Ban the use of cipher suites using DH.
    DHE      Ban the use of cipher suites using authenticated ephemeral DH key agreement.
    ECDH     Ban the use of cipher suites using ECDH key exchange.
    ECDHE    Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.
    DSS      Ban the use of cipher suites using DSS authentication.
    ECDSA    Ban the use of cipher suites using ECDSA authentication.
    AES      Ban the use of cipher suites using either 128 or 256 bit AES.
    AESGCM   Ban the use of cipher suites AES in Galois Counter Mode (GCM).
    CAMELLIA Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.
    3DES     Ban the use of cipher suites using triple DES
    SHA1     Ban the use of cipher suites using SHA1.
    SHA256   Ban the use of cipher suites using SHA256.
    SHA384   Ban the use of cipher suites using SHA384.
    STATIC   Ban the use of cipher suites using static keys.
  set ssl-big-buffer { enable | disable }  Disable using the big SSLv3 buffer feature to save memory and force higher security.
  set ssl-insert-empty-fragment { enable | disable }  Enable/disable insertion of empty fragment.
  set https-redirect { enable | disable }  Enable/disable redirect of port 80 to SSL-VPN port.
  set ssl-client-renegotiation { disable | enable }  Enable to allow client renegotiation by the server if the tunnel goes down.
  set force-two-factor-auth { enable | disable }  Enable to force two-factor authentication for all SSL-VPNs.
  set unsafe-legacy-renegotiation { enable | disable }  Enable/disable unsafe legacy re-negotiation.
  set servercert { string }  Name of the server certificate to be used for SSL-VPNs. size[35] - datasource(s): vpn.certificate.local.name
  set algorithm { high | medium | default | low }  Force the SSL-VPN security level. High allows only high. Medium allows medium and high. Low
allows any.
```

```

        high      High algorithms.
        medium    High and medium algorithms.
        default   default
        low       All algorithms.
set idle-timeout { integer }  SSL VPN disconnects if idle for specified time in seconds. range[0-259200]
set auth-timeout { integer }  SSL-VPN authentication timeout (1 - 259200 sec (3 days), 0 for no timeout). range[0-259200]
set login-attempt-limit { integer }  SSL VPN maximum login attempt times before block (0 - 10, default = 2, 0 = no limit). range[0-4294967295]
set login-block-time { integer }  Time for which a user is blocked from logging in after too many failed login attempts (0 - 86400 sec, default
= 60). range[0-4294967295]
set login-timeout { integer }  SSLVPN maximum login timeout (10 - 180 sec, default = 30). range[10-180]
set dtls-hello-timeout { integer }  SSLVPN maximum DTLS hello timeout (10 - 60 sec, default = 10). range[10-60]
config tunnel-ip-pools
  edit { name }
    # Names of the IPv4 IP Pool firewall objects that define the IP addresses reserved for remote clients.
    set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
config tunnel-ipv6-pools
  edit { name }
    # Names of the IPv6 IP Pool firewall objects that define the IP addresses reserved for remote clients.
    set name { string }  Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
  next
set dns-suffix { string }  DNS suffix used for SSL-VPN clients. size[253]
set dns-server1 { ipv4 address }  DNS server 1.
set dns-server2 { ipv4 address }  DNS server 2.
set wins-server1 { ipv4 address }  WINS server 1.
set wins-server2 { ipv4 address }  WINS server 2.
set ipv6-dns-server1 { ipv6 address }  IPv6 DNS server 1.
set ipv6-dns-server2 { ipv6 address }  IPv6 DNS server 2.
set ipv6-wins-server1 { ipv6 address }  IPv6 WINS server 1.
set ipv6-wins-server2 { ipv6 address }  IPv6 WINS server 2.
set route-source-interface { enable | disable }  Enable to allow SSL-VPN sessions to bypass routing and bind to the incoming interface.
set url-obscuration { enable | disable }  Enable to obscure the host name of the URL of the web browser display.
set http-compression { enable | disable }  Enable to allow HTTP compression over SSL-VPN tunnels.
set http-only-cookie { enable | disable }  Enable/disable SSL-VPN support for HttpOnly cookies.
set deflate-compression-level { integer }  Compression level (0~9). range[0-9]
set deflate-min-data-size { integer }  Minimum amount of data that triggers compression (200 - 65535 bytes). range[200-65535]
set port { integer }  SSL-VPN access port (1 - 65535). range[1-65535]
set port-precedence { enable | disable }  Enable means that if SSL-VPN connections are allowed on an interface admin GUI connections are blocked
on that interface.
set auto-tunnel-static-route { enable | disable }  Enable to auto-create static routes for the SSL-VPN tunnel IP addresses.
set header-x-forwarded-for { pass | add | remove }  Forward the same, add, or remove HTTP header.
  pass      Forward the same HTTP header.
  add       Add the HTTP header.

```

```
        remove Remove the HTTP header.
config source-interface
    edit { name }
        # SSL VPN source interface of incoming traffic.
        set name { string } Interface name. size[35] - datasource(s): system.interface.name,system.zone.name
    next
config source-address
    edit { name }
        # Source address of incoming traffic.
        set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
set source-address-negate { enable | disable } Enable/disable negated source address match.
config source-address6
    edit { name }
        # IPv6 source address of incoming traffic.
        set name { string } IPv6 address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
    next
set source-address6-negate { enable | disable } Enable/disable negated source IPv6 address match.
set default-portal { string } Default SSL VPN portal. size[35] - datasource(s): vpn.ssl.web.portal.name
config authentication-rule
    edit { id }
        # Authentication rule for SSL VPN.
        set id { integer } ID (0 - 4294967295). range[0-4294967295]
        config source-interface
            edit { name }
                # SSL VPN source interface of incoming traffic.
                set name { string } Interface name. size[35] - datasource(s): system.interface.name,system.zone.name
            next
        config source-address
            edit { name }
                # Source address of incoming traffic.
                set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
            next
        set source-address-negate { enable | disable } Enable/disable negated source address match.
        config source-address6
            edit { name }
                # IPv6 source address of incoming traffic.
                set name { string } IPv6 address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
            next
        set source-address6-negate { enable | disable } Enable/disable negated source IPv6 address match.
    config users
        edit { name }
            # User name.
```

```

        set name { string }   User name. size[64] - datasource(s): user.local.name
    next
config groups
    edit { name }
    # User groups.
        set name { string }   Group name. size[64] - datasource(s): user.group.name
    next
set portal { string }   SSL VPN portal. size[35] - datasource(s): vpn.ssl.web.portal.name
set realm { string }   SSL VPN realm. size[35] - datasource(s): vpn.ssl.web.realm.url-path
set client-cert { enable | disable }   Enable/disable SSL VPN client certificate restrictive.
set cipher { any | high | medium }   SSL VPN cipher strength.
    any       Any cipher strength.
    high     High cipher strength ( )= 168 bits).
    medium   Medium cipher strength ( )= 128 bits).
set auth { option }   SSL VPN authentication method restriction.
    any       Any
    local    Local
    radius   RADIUS
    tacacs+  TACACS+
    ldap     LDAP
next
set dtls-tunnel { enable | disable }   Enable DTLS to prevent eavesdropping, tampering, or message forgery.
set check-referer { enable | disable }   Enable/disable verification of referer field in HTTP request header.
set http-request-header-timeout { integer }   SSL-VPN session is disconnected if an HTTP request header is not received within this time (1 - 60
sec, default = 20). range[0-4294967295]
set http-request-body-timeout { integer }   SSL-VPN session is disconnected if an HTTP request body is not received within this time (1 - 60 sec,
default = 20). range[0-4294967295]
end

```

Supplemental Information

The following section is for those commands that require further explanation.

config authentication-rule

A configuration method to create authentication rules for SSL VPN. Edit to create new and specify the rules using the entries available.

reqclientcert {enable | disable}

Enable or disable (by default) the requirement of a client certificate. When enabled, the SSL VPN daemon will require a client certificate for all SSL VPN users, regardless of policy.

sslv3 {enable | disable}

Enable or disable (by default) SSLv3.

SSLv3 is no longer commonly used, and it is recommended to not use this security measure.

tlsv1-0 {enable | disable}

Enable or disable (by default) Transport Layer Security (TLS) version 1.0 (TLSv1.0).

tlsv1-1 {enable | disable}

Enable (by default) or disable TLSv1.1.

tlsv1-2 {enable | disable}

Enable (by default) or disable TLSv1.2, currently the most recent version.

banned-cipher <cipher>

Banned ciphers for SSL VPN. Set one or more of the following to ban the use of cipher suites using:

- **RSA:** Rivest-Shamir-Adleman key
- **DH:** Diffie Hellman
- **DHE:** Authenticated ephemeral DH key agreement
- **ECDH:** Elliptic Curve DH key exchange
- **ECDHE:** Authenticated ephemeral ECDH key agreement
- **DSS:** Digital Signature Standard authentication

- **ECDSA:** Elliptic Curve Digital Signature Algorithm authentication
- **AES:** Advanced Encryption Standard, either 128 or 256 bit
- **AESGCM:** AES in Galois Counter Mode
- **CAMELLIA:** A symmetric block cipher algorithm, either 128 or 256 bit
- **3DES:** Triple Data Encryption Standard
- **SHA1:** 160 bit Secure Hash Algorithm
- **SHA256:** 256 bit SHA
- **SHA384:** 384 bit SHA

ssl-big-buffer {enable | disable}

Enable or disable (by default) big SSLv3 buffer used for communicating with older applications that do not use standard SSL record sizes. When disabled, memory use is reduced by approximately 16kb per connection.

ssl-insert-empty-fragment {enable | disable}

Enable (by default) or disable the insertion of empty fragments, a counter measure to avoid Browser Exploit Against SSL/TLS (BEAST) attacks.

https-redirect {enable | disable}

Enable or disable (by default) the redirection of port 80 to the SSL VPN port.

ssl-client-renegotiation {enable | disable}

Enable (allow) or disable (block, by default) client renegotiation by the server if the tunnel goes down.

force-two-factor-auth {enable | disable}

Enable or disable (by default) the imposition of two-factor authentication. When enabled, PKI (peer) users will be required to authenticate with their password and certificate authentication. In addition, only PKI users with two-factor authentication enabled will be able to log on to the SSL VPN.

servercert <cert-name>

The server's certificate used to identify the FortiGate unit during the SSL handshake with a web browser when the web browser connects to the login page. The certificate must have already been configured on the FortiGate before entering it here. The default is set to `Fortinet_Factory`.

algorithm {high | medium | low}

Force the SSL VPN security level. `high` allows only high security algorithms. `medium` allows medium and high. `low` allows any.

idle-timeout <timeout>

The period of time in seconds that the SSL VPN will wait before timing out. Set the value between 1-259200 (or 1 second to 3 days), or 0 for no timeout. The default is set to 300.

auth-timeout <timeout>

The period of time in seconds that the SSL VPN will wait before re-authentication is enforced. Set the value between 1-259200 (or 1 second 3 days), or 0 for no timeout. The default is set to 28800.

{tunnel-ip-pools | tunnel-ipv6-pools} <pool-name>

The tunnel IPv4 or IPv6 pools reserved for remote clients. The addresses and address groups must have already been configured on the FortiGate unit before entering them here.

dns-suffix <string>

The DNS suffix, with a maximum length of 253 characters.

{dns-server1 | ipv6-dns-server1} <addr-ip4/6>

The IPv4 or IPv6 IP address of the primary DNS server that SSL VPN clients will be able to access after a connection has been established. Use the `dns-server2` or `ipv6-dns-server-2` entries to specify a secondary DNS server (see entry below).

{dns-server2 | ipv6-dns-server2} <addr-ip4/6>

The IPv4 or IPv6 IP address of the secondary DNS server that SSL VPN clients will be able to access after a connection has been established.

{wins-server1 | ipv6-wins-server1} <addr-ip4/6>

The IPv4 or IPv6 IP address of the primary WINS server that SSL VPN clients will be able to access after a connection has been established. Use the `wins-server2` or `ipv6-wins-server2` entries to specify a secondary WINS server (see entry below).

{wins-server2 | ipv6-wins-server2} <addr-ip4/6>

The IPv4 or IPv6 IP address of the secondary WINS server that SSL VPN clients will be able to access after a connection has been established.

route-source-interface {enable | disable}

Enable or disable (by default) allowing SSL VPN connections to bypass routing and bind to the incoming interface.

url-obscuration {enable | disable}

Enable or disable (by default) encryption of the host name of the URL in the display (web address) of the web browser (for web mode only).

Enabling this feature is required for International Computer Security Association (ICSA) SSL VPN certification. Note that, when enabled, bookmark details are not visible.

http-compression {enable | disable}

Enable or disable (by default) the use of compression between the FortiGate unit and the client web browser. When enabled, use the `deflate-compression-level` and `deflate-min-data-size` entries to tune performance (see entries below).

http-only-cookie {enable | disable}

Enable (by default) or disable SSL VPN support for [HttpOnly](#) cookies.

deflate-compression-level <integer>

Note: This entry is only available when `http-compression` is set to `enable`.

The compression level. Set the value between 1-9. Higher compression values reduce the volume of data but requires more processing time. The default is set to 6.

deflate-min-data-size <integer>

Note: This entry is only available when `http-compression` is set to `enable`.

The minimum amount of data in bytes that will trigger compression. Set the value between 200-65535. The default is set to 300.

port <integer>

The SSL VPN access port. Set the value between 1-65535. When VDOMs are enabled, this feature is set per VDOM. The default value is set to 10443.

port-precedence {enable | disable}

Use this command to control how the FortiGate handles a connection attempt if there is a conflict between administrator access to the GUI and to SSL VPN. This can happen if both SSL VPN and HTTPS admin GUI access use the same port on the same FortiGate interface. When this happens, if `port-precedence` is enabled when an HTTPS connection attempt is received on an interface with an SSL VPN portal the FortiGate assumes its an SSL VPN connection attempt and admin GUI access is not allowed. If `port-precedence` is disabled the FortiGate assumes its an admin GUI access attempt and SSL VPN access is not allowed.

Enabled by default.

auto-tunnel-static-route {enable | disable}

Enable (by default) or disable the automatic creation of static routes for the networks that can be accessed through the SSL VPN tunnel. This is only possible if tunnel mode is enabled.

header-x-forwarded-for {pass | add | remove}

Action when HTTP x-forwarded-for header to forwarded requests.

- `pass` forwards the same HTTP header.
 - `add` (by default) adds the HTTP header.
 - `remove` removes the HTTP header.
-

source-interface <interface>

The interface(s) to listen on for SSL clients. You must have already configured the interfaces on the FortiGate unit before entering them here. Enter `any` to match any interface in the virtual domain.

{source-address | source-address6} [addr-ip4/6]

An optional feature to specify IPv4 or IPv6 addresses from which users can log in. Leave this entry blank to allow login from any address.

{source-address-negate | source-address6-negate} {enable | disable}

Enable or disable {by default} inverting the `source-address` or `source-address6` entries so that it instead specifies IPv4 or IPv6 addresses to not allow.

default-portal <portal-name>

The name of the default SSL VPN portal, either one of the defaults (`full-access`, `tunnel-access`, or `web-access`) or a custom portal created on the FortiGate unit.

dtls-tunnel {enable | disable}

Enable (by default) or disable the Datagram Transport Layer Security (DTLS) tunnel, allowing datagram-based applications to communicate in a way that prevents eavesdropping, tampering, or message forgery.

check-referer {enable | disable}

Enable or disable (by default) the verification of referer field in HTTP request header.

http-request-header-timeout <timeout>

The amount of time in seconds before the HTTP connection disconnects if HTTP request header is not complete. Set value between 1-60 (or one second to one minute). The default is set to 20.

http-request-body-timeout <timeout>

The amount of time in seconds before the HTTP connection disconnects if HTTP request body is not complete. Set value between 1-60 (or one second to one minute). The default is set to 30.

vpn ssl web host-check-software

Use this command to define the Windows Firewall software and add your own software requirements to the host check list.

Note: Host integrity checking is only possible with client computers running Microsoft Windows platforms.

```
config vpn ssl web host-check-software
  edit { name }
    # SSL-VPN host check software.
    set name { string } Name. size[63]
    set type { av | fw } Type.
      av AntiVirus.
      fw Firewall.
    set version { string } Version. size[35]
    set guid { string } Globally unique ID.
    config check-item-list
      edit { id }
        # Check item list.
        set id { integer } ID (0 - 4294967295). range[0-65535]
        set action { require | deny } Action.
          require Require.
          deny Deny.
        set type { file | registry | process } Type.
          file File.
          registry Registry.
          process Process.
        set target { string } Target. size[255]
        set version { string } Version. size[35]
        config md5s
          edit { id }
            # MD5 checksum.
            set id { string } Hex string of MD5 checksum. size[32]
          next
        next
      next
    end
```


Supplemental Information

The following section is for those commands that require further explanation.

config check-item-list

A configuration method to set various check item list variables. Edit to create new and configure settings using the following entries.

action {require | deny}

The course of action taken when the item is found.

- `require`: If the item is found, the client meets the check item condition. This is the default option.
 - `deny`: If the item is found, the client is considered to not meet the check item condition. Use this option if it is necessary to prevent the use of a particular security product.
-

type {file | registry | process}

The method used to check for the application.

- `file`: Looks for any file that would confirm the presence of the application, not just the application's executable file. This is the default option. Once set, use the `target` entry below and set it to the full path to the file. Where applicable, you can use environment variables enclosed in percent (%) marks, e.g. `%ProgramFiles%\Fortinet\FortiClient\FortiClient.exe`.
 - `registry`: Looks for a Windows Registry entry. Once set, use the `target` entry below and set it to the registry item, e.g. `HKLM\SOFTWARE\Fortinet\FortiClient\Misc`.
 - `process`: Looks for the application as a running process. Once set, use the `target` entry below and set it to the application's executable file name.
-

target <target>

Depending on what the type entry above is set to, set `target` as follows:

- If type is `file`, enter the full path to the file.
- If type is `registry`, enter the registry item.

- If type is `process`, enter the application's executable file name.
-

version <version>

Enter the application version.

md5s <md5s>

If type is set to file or process, this entry can be used to enter one or more known MD5 signatures for the application's executable file. You can use a third-party utility to calculate MD5 signatures or hashes for any file. In addition, you can enter multiple signatures to match multiple versions of the application.

type {av | fw}

The software type, antivirus (`av`, set by default) or firewall (`fw`). If the software does both, create two separate entries and assign each entry with a type.

version <version-number>

Enter the software version.

guid <guid-value>

Enter the globally unique identifier (GUID) for the host check application. The value is a hexadecimal number, usually in the form `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx`. Windows uses GUIDs to identify applications in the Windows Registry.

vpn ssl web portal

Use this command to configure the SSL VPN portal service, allowing you to access network resources through a secure channel using a web browser. Administrators can configure login privileges for users and define which network resources are available to the users, including HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP, and SSH.

The portal configuration determines what the user sees when they log in to the FortiGate. Both the administrator and the user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- **full-access:** Includes all widgets available to the user – Session Information, Connection Tool, Bookmarks, and Tunnel Mode.
- **tunnel-access:** Includes Session Information and Tunnel Mode widgets.
- **web-access:** Includes Session Information and Bookmarks widgets.

```
config vpn ssl web portal
  edit { name }
    # Portal.
    set name { string } Portal name. size[35]
    set tunnel-mode { enable | disable } Enable/disable IPv4 SSL-VPN tunnel mode.
    set ip-mode { range | user-group } Method by which users of this SSL-VPN tunnel obtain IP addresses.
      range Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.
      user-group Use IP the addresses associated with individual users or user groups (usually from external auth servers).
    set auto-connect { enable | disable } Enable/disable automatic connect by client when system is up.
    set keep-alive { enable | disable } Enable/disable automatic reconnect for FortiClient connections.
    set save-password { enable | disable } Enable/disable FortiClient saving the user's password.
  config ip-pools
    edit { name }
      # IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients.
      set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
  set exclusive-routing { enable | disable } Enable/disable all traffic go through tunnel only.
  set service-restriction { enable | disable } Enable/disable tunnel service restriction.
  set split-tunneling { enable | disable } Enable/disable IPv4 split tunneling.
  config split-tunneling-routing-address
    edit { name }
      # IPv4 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling
  access.
```

```

        set name { string }   Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
set dns-server1 { ipv4 address }   IPv4 DNS server 1.
set dns-server2 { ipv4 address }   IPv4 DNS server 2.
set dns-suffix { string }   DNS suffix. size[253]
set wins-server1 { ipv4 address }   IPv4 WINS server 1.
set wins-server2 { ipv4 address }   IPv4 WINS server 1.
set ipv6-tunnel-mode { enable | disable }   Enable/disable IPv6 SSL-VPN tunnel mode.
config ipv6-pools
    edit { name }
        # IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients.
        set name { string }   Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
    next
set ipv6-exclusive-routing { enable | disable }   Enable/disable all IPv6 traffic go through tunnel only.
set ipv6-service-restriction { enable | disable }   Enable/disable IPv6 tunnel service restriction.
set ipv6-split-tunneling { enable | disable }   Enable/disable IPv6 split tunneling.
config ipv6-split-tunneling-routing-address
    edit { name }
        # IPv6 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling
access.
        set name { string }   Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
    next
set ipv6-dns-server1 { ipv6 address }   IPv6 DNS server 1.
set ipv6-dns-server2 { ipv6 address }   IPv6 DNS server 2.
set ipv6-wins-server1 { ipv6 address }   IPv6 WINS server 1.
set ipv6-wins-server2 { ipv6 address }   IPv6 WINS server 2.
set web-mode { enable | disable }   Enable/disable SSL VPN web mode.
set display-bookmark { enable | disable }   Enable to display the web portal bookmark widget.
set user-bookmark { enable | disable }   Enable to allow web portal users to create their own bookmarks.
set allow-user-access { option }   Allow user access to SSL-VPN applications.
    web           HTTP/HTTPS access.
    ftp           FTP access.
    smb           SMB/CIFS access.
    telnet        TELNET access.
    ssh           SSH access.
    vnc           VNC access.
    rdp           RDP access.
    ping          PING access.
    citrix        CITRIX access.
    portforward   Port Forward access.
set user-group-bookmark { enable | disable }   Enable to allow web portal users to create bookmarks for all users in the same user group.
config bookmark-group
    edit { name }

```

```
# Portal bookmark group.
set name { string } Bookmark group name. size[35]
config bookmarks
edit { name }
# Bookmark table.
set name { string } Bookmark name. size[35]
set apptype { option } Application type.
    citrix      Citrix.
    ftp         FTP.
    portforward Port Forward.
    rdp         RDP.
    smb         SMB/CIFS.
    ssh         SSH.
    telnet      Telnet.
    vnc         VNC.
    web         HTTP/HTTPS.
set url { string } URL parameter. size[128]
set host { string } Host name/IP parameter. size[128]
set folder { string } Network shared file folder parameter. size[128]
set additional-params { string } Additional parameters. size[128]
set listening-port { integer } Listening port (0 - 65535). range[0-65535]
set remote-port { integer } Remote port (0 - 65535). range[0-65535]
set show-status-window { enable | disable } Enable/disable showing of status window.
set description { string } Description. size[128]
set server-layout { option } Server side keyboard layout.
    en-us-qwerty English (US) keyboard
    de-de-qwertz German keyboard (qwertz)
    fr-fr-azerty French keyboard (azerty)
    it-it-qwerty Italian keyboard
    sv-se-qwerty Swedish keyboard
    failsafe     Unknown keyboard
set security { rdp | nla | tls | any } Security mode for RDP connection.
    rdp Standard RDP encryption.
    nla Network Level Authentication.
    tls TLS encryption.
    any Allow the server to choose the type of security.
set port { integer } Remote port. range[0-65535]
set logon-user { string } Logon user. size[35]
set logon-password { password_string } Logon password. size[128]
set sso { disable | static | auto } Single Sign-On.
    disable Disable SSO.
    static Static SSO.
    auto Auto SSO.
```

```

    config form-data
        edit { name }
            # Form data.
            set name { string }    Name. size[35]
            set value { string }   Value. size[63]
        next
    set sso-credential { sslvpn-login | alternative }    Single sign-on credentials.
        sslvpn-login    SSL-VPN login.
        alternative     Alternative.
    set sso-username { string }    SSO user name. size[35]
    set sso-password { password_string }    SSO password. size[128]
next
next
set display-connection-tools { enable | disable }    Enable to display the web portal connection tools widget.
set display-history { enable | disable }    Enable to display the web portal user login history widget.
set display-status { enable | disable }    Enable to display the web portal status widget.
set heading { string }    Web portal heading message. size[31]
set redir-url { string }    Client login redirect URL. size[255]
set theme { option }    Web portal color scheme.
    blue        Light blue theme.
    green       Green theme.
    red         Red theme.
    melongene   Melongene theme (eggplant color).
    mariner     Mariner theme (dark blue color).
set custom-lang { string }    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. size[35] - datasource(s): system.custom-language.name
set smb-ntlmv1-auth { enable | disable }    Enable support of NTLMv1 for Samba authentication.
set host-check { option }    Type of host checking performed on endpoints.
    none        No host checking.
    av          AntiVirus software recognized by the Windows Security Center.
    fw          Firewall software recognized by the Windows Security Center.
    av-fw       AntiVirus and firewall software recognized by the Windows Security Center.
    custom      Custom.
set host-check-interval { integer }    Periodic host check interval. Value of 0 means disabled and host checking only happens when the end-
point connects. range[120-259200]
config host-check-policy
    edit { name }
        # One or more policies to require the endpoint to have specific security software.
        set name { string }    Host check software list name. size[64] - datasource(s): vpn.ssl.web.host-check-software.name
    next
set limit-user-logins { enable | disable }    Enable to limit each user to one SSL-VPN session at a time.
set mac-addr-check { enable | disable }    Enable/disable MAC address host checking.
set mac-addr-action { allow | deny }    Client MAC address action.

```

```
        allow Allow connection when client MAC address is matched.
        deny Deny connection when client MAC address is matched.
config mac-addr-check-rule
    edit { name }
        # Client MAC address check rule.
        set name { string } Client MAC address check rule name. size[35]
        set mac-addr-mask { integer } Client MAC address mask. range[1-48]
        config mac-addr-list
            edit { addr }
                # Client MAC address list.
                set addr { mac address } Client MAC address.
            next
        next
set os-check { enable | disable } Enable to let the FortiGate decide action based on client OS.
config os-check-list
    edit { name }
        # SSL VPN OS checks.
        set name { string } Name. size[15]
        set action { deny | allow | check-up-to-date } OS check options.
            deny Deny all OS versions.
            allow Allow any OS version.
            check-up-to-date Verify OS is up-to-date.
        set tolerance { integer } OS patch level tolerance. range[0-255]
        set latest-patch-level { string } Latest OS patch level.
    next
set forticlient-download { enable | disable } Enable/disable download option for FortiClient.
set forticlient-download-method { direct | ssl-vpn } FortiClient download method.
    direct Download via direct link.
    ssl-vpn Download via SSL-VPN.
set customize-forticlient-download-url { enable | disable } Enable support of customized download URL for FortiClient.
set windows-forticlient-download-url { string } Download URL for Windows FortiClient. size[1023]
set macos-forticlient-download-url { string } Download URL for Mac FortiClient. size[1023]
set skip-check-for-unsupported-os { enable | disable } Enable to skip host check if client OS does not support it.
set skip-check-for-unsupported-browser { enable | disable } Enable to skip host check if browser does not support it.
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

reqclientcert {enable | disable}

Enable or disable (by default) the requirement of a client certificate. When enabled, the SSL VPN daemon will require a client certificate for all SSL VPN users, regardless of policy.

{tunnel-mode | ipv6-tunnel-mode} {enable | disable}

Enable (by default) or disable IPv4 or IPv6 tunnel mode.

ip-mode {range | usrgrp}

Note: This entry is only available when `tunnel-mode` is set to `enable`.

How users of this SSL VPN tunnel get IP addresses:

- `range` use the IP addresses available for all SSL VPN users as defined by the `config vpn ssl settings` command.
 - `user-group` use IP addresses associated with individual users or user groups (usually from external authentication servers (such as RADIUS, LDAP, etc.).
-

auto-connect {enable | disable}

Note: This entry is only available when either `tunnel-mode` or `ipv6-tunnel-mode` is set to `enable`.

Enable or disable (by default) FortiClient automatic connection when the system is up.

keep-alive {enable | disable}

Note: This entry is only available when either `tunnel-mode` or `ipv6-tunnel-mode` is set to `enable`.

Enable or disable (by default) the automatic reconnection for FortiClient connections by the client.

save-password {enable | disable}

Note: This entry is only available when either `tunnel-mode` or `ipv6-tunnel-mode` is set to `enable`.

Enable or disable (by default) FortiClient saving the user's password.

{ip-pools | ipv6-pools} <pool-names>

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The names of the IPv4 or IPv6 firewall address objects reserved for SSL VPN tunnel mode clients.

{split-tunneling | ipv6-split-tunneling} {enable | disable}

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

Enable (by default) or disable IPv4 or IPv6 split tunneling, ensuring that only the traffic for the private network is sent to the SSL VPN gateway.

{split-tunneling-routing-address | ipv6-split-tunneling-routing-address} <address-name>

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

IPv4 or IPv6 SSL VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access.

{dns-server1 | ipv6-dns-server1} <addr-ip4/6>

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the primary DNS server that SSL VPN clients will be able to access after a connection has been established. Use the `dns-server2` or `ipv6-dns-server-2` entries to specify a secondary DNS server (see entry below).

{dns-server2 | ipv6-dns-server2} <addr-ip4/6>

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the secondary DNS server that SSL VPN clients will be able to access after a connection has been established.

{wins-server1 | ipv6-wins-server1} <addr-ip4/6>

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the primary WINS server that SSL VPN clients will be able to access after a connection has been established. Use the `wins-server2` or `ipv6-wins-server2` entries to specify a secondary WINS server (see entry below).

{wins-server2 | ipv6-wins-server2}

Note: These entries are only available when `tunnel-mode` or `ipv6-tunnel-mode` are set to `enable`.

The IPv4 or IPv6 IP address of the secondary WINS server that SSL VPN clients will be able to access after a connection has been established.

web-mode {enable | disable}

Enable or disable (by default) web mode.

display-bookmark {enable | disable}

Note: This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web mode bookmark widget.

user-bookmark {enable | disable}

Note: This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable allowing web portal users to create their own bookmarks.

user-group-bookmark {enable | disable}

Note: This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable allowing web portal users to create bookmarks for all users in the same user group.

display-connection-tools {enable | disable}

Note: This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web portal connection tools widget.

display-history {enable | disable}

Note: This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web portal user login history widget.

display-status {enable | disable}

Note: This entry is only available when `web-mode` is set to `enable`.

Enable (by default) or disable the web portal status widget.

heading <message>

The portal heading message.

redir-url <url>

Note: This entry is only available when `web-mode` is set to `enable`.

The URL of the web page that enables the FortiGate to display a second HTML page when the web portal home page is displayed. The web server for this URL must reside on the private network behind the FortiGate unit.

theme <colour>

Note: This entry is only available when `web-mode` is set to `enable`.

The web portal color scheme: `blue` (by default), `gray`, or `orange`.

custom-lang <language>

Note: This entry is only available when `web-mode` is set to `enable`.

Change the display language for this web portal. Select from the following options. The options are named according to the config system `custom-language` command that you can use to customize the content of these language files. By default the content of these language files is provided by Fortinet in the languages listed below.

- `GB2312`: Simplified Chinese (using the Guojia Biao zhun (GB), or 'national standard' in Chinese, is the registered character set of the People's Republic of China used for Simplified Chinese characters).
- `big5`: Traditional Chinese (using Big5, or Big-5, is a Chinese character encoding method used in Taiwan, Hong Kong, and Macau for Traditional Chinese characters).
- `en`: English (using the English character set (Caribbean)).
- `euc-kr`: Korean (using the Wxtended Unix Code (EUC) is a character encoding system used for Japanese, Korean, and Simplified Chinese. This featured option is specifically for Korean).
- `fr`: French (Using the French character set (Standard)).
- `pg`: Portuguese (Using the Proto-Germanic (PG), also called Common Germanic, character set).
- `sp`: Spanish (using the Spanish character set).
- `x-sjis`: Japanese (using the Shift Japanese Industrial Standards (SJIS), is a character encoding method for Japanese).

host-check {none | av | fw | av-fw | custom}

The type of host checking to perform on endpoints.

- `none`: Do not perform host checking.
- `av`: Check for antivirus software recognized by the Windows Security Center.
- `fw`: Check for firewall software recognized by the Windows Security Center.
- `av-fw`: Check for both antivirus and firewall software recognized by the Windows Security Center.
- `custom`: Check for the software defined in the `host-check-policy` entry.

host-check-interval <seconds>

How often the host check function periodically verifies the host check status of endpoints. Range is 120 to 259200 seconds. Default is 0, which disables periodic host checking. If disabled host checking only happens when the endpoint initially connects to the SSL VPN. Only available if `host-check` is enabled.

host-check-policy {<policy> [<policy>...]}

Select one or more host-check policy to perform different types of host checking. You can use this option to add a wide range of host checking options to require endpoints to have a wide range of security software. You can see the complete list of host check policies and add more using the [config vpn ssl host-check-software](#) command.

This option is available when `host-check` is set to `custom`.

limit-user-logins {enable | disable}

Enable or disable (by default) permitting each user one SSL VPN session at a time.

mac-addr-check {enable | disable}

Enable or disable (by default) MAC address host checking.

os-check {enable | disable}

Enable or disable (by default) the FortiGate unit to determine what action to take depending on what operating system the client has.

skip-check-for-unsupported-os {enable | disable}

Note: This entry is only available when either `os-check` or `virtual-desktop` is set to `enable`.

Enable (by default) or disable skipping the host check if the client operating system doesn't support it.

skip-check-for-unsupported-browser {enable | disable}

Note: This entry is only available when either `os-check` or `virtual-desktop` is set to `enable`.

Enable (by default) or disable skipping the host check if the browser doesn't support it.

virtual-desktop {enable | disable}

Enable or disable (by default) the SSL VPN virtual desktop client application. If enabled on the client, attempted connections via SSL VPN are refused.

virtual-desktop-app-list <name>

Note: This entry is only available when `virtual-desktop` is set to `enable`.

The name of the application list to apply to the virtual desktop (for more information see the [vpn ssl web virtual-desktop-app-list](#) command).

virtual-desktop-clipboard-share {enable | disable}

Note: This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) sharing of the clipboard with the regular desktop.

virtual-desktop-desktop-switch {enable | disable}

Note: This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) switching between virtual and regular desktop.

virtual-desktop-logout-when-browser-close {enable | disable}

Note: This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) automatic logout from virtual desktop when browser is closed.

virtual-desktop-network-share-access {enable | disable}

Note: This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) network share access from the virtual desktop.

virtual-desktop-printing {enable | disable}

Note: This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) printing from the virtual desktop.

virtual-desktop-removable-media-access {enable | disable}

Note: This entry is only available when `virtual-desktop` is set to `enable`.

Enable or disable (by default) accessing removable media such as USB drives from the virtual desktop.

vpn ssl web realm

Use this command to configure SSL VPN realms. Use this command to customize the SSL VPN login page for your users, and also create multiple SSL VPN logins for different user groups.

Note: When you edit a realm, the name entered is the URL path used to access the SSL VPN login page (do *not* include `http://`).

```
config vpn ssl web realm
  edit { url-path }
  # Realm.
  set url-path { string }   URL path to access SSL-VPN login page. size[35]
  set max-concurrent-user { integer }   Maximum concurrent users (0 - 65535, 0 means unlimited). range[0-65535]
  set login-page { string }   Replacement HTML for SSL-VPN login page. size[32768]
  set virtual-host { string }   Virtual host name for realm. size[255]
  next
end
```

max-concurrent-user <number>

The maximum number of concurrent users. Set the value between 1-65535, or 0 (by default) for unlimited users.

login-page <content>

Replacement HTML for the SSL VPN login page.

virtual-host [host-name]

The virtual host name for the realm (optional), with a maximum length of 255 characters.

vpn ssl web user-bookmark

Introduction.

```
config vpn ssl web user-bookmark
  edit { name }
  # Configure SSL VPN user bookmark.
  set name { string }  User and group name. size[101]
  set custom-lang { string }  Personal language. size[35] - datasource(s): system.custom-language.name
  config bookmarks
  edit { name }
  # Bookmark table.
  set name { string }  Bookmark name. size[35]
  set apptype { option }  Application type.
    citrix      Citrix.
    ftp         FTP.
    portforward Port Forward.
    rdp         RDP.
    smb        SMB/CIFS.
    ssh        SSH.
    telnet     Telnet.
    vnc        VNC.
    web        HTTP/HTTPS.
  set url { string }  URL parameter. size[128]
  set host { string }  Host name/IP parameter. size[128]
  set folder { string }  Network shared file folder parameter. size[128]
  set additional-params { string }  Additional parameters. size[128]
  set listening-port { integer }  Listening port (0 - 65535). range[0-65535]
  set remote-port { integer }  Remote port (0 - 65535). range[0-65535]
  set show-status-window { enable | disable }  Enable/disable showing of status window.
  set description { string }  Description. size[128]
  set server-layout { option }  Server side keyboard layout.
    en-us-qwerty English (US) keyboard
    de-de-qwertz German keyboard (qwertz)
    fr-fr-azerty French keyboard (azerty)
    it-it-qwerty Italian keyboard
    sv-se-qwerty Swedish keyboard
    failsafe    Unknown keyboard
  set security { rdp | nla | tls | any }  Security mode for RDP connection.
```

```
        rdp Standard RDP encryption.
        nla Network Level Authentication.
        tls TLS encryption.
        any Allow the server to choose the type of security.
set port { integer } Remote port. range[0-65535]
set logon-user { string } Logon user. size[35]
set logon-password { password_string } Logon password. size[128]
set sso { disable | static | auto } Single Sign-On.
        disable Disable SSO.
        static Static SSO.
        auto Auto SSO.
config form-data
    edit { name }
        # Form data.
        set name { string } Name. size[35]
        set value { string } Value. size[63]
    next
set sso-credential { sslvpn-login | alternative } Single sign-on credentials.
        sslvpn-login SSL-VPN login.
        alternative Alternative.
set sso-username { string } SSO user name. size[35]
set sso-password { password_string } SSO password. size[128]
next
next
end
```

vpn ssl web user-group-bookmark

Use this command to add bookmarks that will appear on the SSL VPN web portal for all of the users in a user group.

```
config vpn ssl web user-group-bookmark
  edit { name }
  # Configure SSL VPN user group bookmark.
  set name { string }  Group name. size[64] - datasource(s): user.group.name
  config bookmarks
    edit { name }
    # Bookmark table.
    set name { string }  Bookmark name. size[35]
    set apptype { option }  Application type.
      citrix      Citrix.
      ftp         FTP.
      portforward Port Forward.
      rdp         RDP.
      smb         SMB/CIFS.
      ssh         SSH.
      telnet      Telnet.
      vnc         VNC.
      web         HTTP/HTTPS.
    set url { string }  URL parameter. size[128]
    set host { string }  Host name/IP parameter. size[128]
    set folder { string }  Network shared file folder parameter. size[128]
    set additional-params { string }  Additional parameters. size[128]
    set listening-port { integer }  Listening port (0 - 65535). range[0-65535]
    set remote-port { integer }  Remote port (0 - 65535). range[0-65535]
    set show-status-window { enable | disable }  Enable/disable showing of status window.
    set description { string }  Description. size[128]
    set server-layout { option }  Server side keyboard layout.
      en-us-qwerty English (US) keyboard
      de-de-qwertz German keyboard (qwertz)
      fr-fr-azerty French keyboard (azerty)
      it-it-qwerty Italian keyboard
      sv-se-qwerty Swedish keyboard
      failsafe    Unknown keyboard
    set security { rdp | nla | tls | any }  Security mode for RDP connection.
      rdp Standard RDP encryption.
```

```

        nla Network Level Authentication.
        tls TLS encryption.
        any Allow the server to choose the type of security.
set port { integer } Remote port. range[0-65535]
set logon-user { string } Logon user. size[35]
set logon-password { password_string } Logon password. size[128]
set sso { disable | static | auto } Single Sign-On.
    disable Disable SSO.
    static Static SSO.
    auto Auto SSO.
config form-data
    edit { name }
        # Form data.
        set name { string } Name. size[35]
        set value { string } Value. size[63]
    next
set sso-credential { sslvpn-login | alternative } Single sign-on credentials.
    sslvpn-login SSL-VPN login.
    alternative Alternative.
set sso-username { string } SSO user name. size[35]
set sso-password { password_string } SSO password. size[128]
next
next
end

```

config bookmarks

A configuration method to configure bookmarks to add to the user group.

apptype {citrix | ftp | portforward | rdp | smb | ssh | telnet | vnc | web}

The identifier of the service to associate with the bookmark.

- `citrix`: Citrix web server interface
- `ftp`: FTP services
- `portforward`: port forwarding
- `rdp`: Windows Terminal services
- `smb`: SMB/CIFS (Windows file share) services

- `ssh`: SSH services
 - `telnet`: telnet services
 - `vnc`: VNC services
 - `web`: HTTP/HTTPS services (this is set by default)
-

folder <folder>

Note: This entry is only available when `apptype` is set to either `ftp` or `smb`.

The folder path.

host <host>

Note: This entry is only available when `apptype` is set to either `portforward`, `rdp`, `ssh`, `telnet`, or `vnc`.

The host IP address or FQDN.

listening-port <port-number>

Note: This entry is only available when `apptype` is set to `portforward`.

The listening port, set to 0 by default.

remote-port <port-number>

Note: This entry is only available when `apptype` is set to `portforward`.

The remote port, set to 0 by default.

show-status-window {enable | disable}

Note: This entry is only available when `apptype` is set to `portforward`.

Enable or disable (by default) the status window display.

url <url>

The URL for this bookmark.

description <description>

The description of the bookmark, with a maximum length of 129 characters.

server-layout {en-us-qwerty | de-de-qwertz | fr-fr-azerty | it-it-qwerty | sv-se-qwerty | failsafe}

Note: This entry is only available when `apptype` is set to `rdp`. Also note that this entry is called `keyboard-layout` in FortiOS 5.2.

The keyboard layout. Select from a number of different layouts.

- `en-us-qwerty`: The American-English QWERTY layout. This is set by default.
 - `de-de-qwertz`: The Deutsch QWERTZ layout.
 - `fr-fr-azerty`: The French AZERTY layout.
 - `it-it-qwerty`: The Italian QWERTY layout.
 - `sv-se-qwerty`: The Swedish QWERTY layout.
 - `failsafe`: Forces all keyboard events to be sent as Unicode.
-

security {rdp | nla | tls | any}

Note: This entry is only available when `apptype` is set to `rdp`.

The type of encryption security.

- `rdp`: Standard RDP encryption (set by default)
 - `nla`: Network Level Authentication (NLA)
 - `tls`: TLS encryption
 - `any`: Allow the server to choose the type of security.
-

port <integer>

Note: This entry is only available when `apptype` is set to either `rdp` or `vnc`.

The remote port. Set the value between 1-65535. The default value is set to 3389.

logon-user <name>

Note: This entry is only available when `apptype` is set to `rdp`.

The name of the user.

logon-password <password>

Note: This entry is only available when `apptype` is set to either `rdp` or `vnc`.

The user's password.

sso {disable | static | auto}

A Single-Sign On (SSO) bookmark that automatically enters the login credentials for the bookmark destination.

- `disable`: This is not an SSO bookmark
 - `static`: This is an SSO bookmark
 - `auto`: Determines whether SSO is used or not automatically
-

sso-credential {sslvpn-login | alternative}

Note: This entry is only available when `sso` is set to either `static` or `auto`.

How the user's credentials are submitted.

- `sslvpn-login`: The bookmark enters the user's SSL VPN credentials.
 - `alternative`: Alternative credentials are given, as defined in the `sso-username` and `sso-password` entries (see below).
-

sso-username <name>

Note: This entry is only available when `sso-credential` is set to `alternative`.

The user's alternative username.

sso-password <password>

Note: This entry is only available when `sso-credential` is set to `alternative`.

The user's alternative password.

config form-data

Note: This configuration option is only available when `sso` is set to `static`.

A configuration method to set form data values. Edit to create new and specify the settings using the entry available. When configuring an entry, as an administrator configuring bookmarks for users, enter `%username%` to represent the user's SSL VPN user name. Enter `%passwd%` to represent the user's password.

vpn ssl web virtual-desktop-app-list

Use this command to create a list of either allowed or blocked applications which can be used when configuring the virtual desktop.

```
config vpn ssl web virtual-desktop-app-list
  edit { name }
  # SSL-VPN virtual desktop application list.
  config apps
    edit { name }
    # Applications.
    config md5s
      edit { id }
      # MD5 checksum.
      set id { string } Hex string of MD5 checksum. size[32]
    next
    set name { string } Name. size[35]
  next
  set action { allow | block } Action.
    allow Allow.
    block Block.
  set name { string } Application list name. size[35]
next
end
```

action {allow | block}

The action to take for this application control list.

- **allow:** Allows the applications on this list and blocks all others. This is set by default.
- **block:** Blocks the applications on this list and allows all others.

config apps

A configuration method of adding the name of the application(s) to be added to this application control list. This can be any name and does not have to match the official name of the application. Edit to create new and specify the applications.

md5s

A configuration method, within config apps, of entering one or more known MD5 signatures for the application's executable file. Separate each signature with a space. You can use a third-party utility to calculate MD5 signatures or hashes for any file. In addition, you can enter multiple signatures to match multiple versions of the application. Edit to create new and specify the signatures.

waf

Introduction.

This section includes syntax for the following commands:

- [waf main-class](#)
- [waf profile](#)
- [waf signature](#)
- [waf sub-class](#)

waf main-class

Introduction.

```
config waf main-class
  edit { id }
  # Hidden table for datasource.
  set name { string }  Main signature class name. size[127]
  set id { integer }   Main signature class ID. range[0-4294967295]
  next
end
```

waf profile

Introduction.

```
config waf profile
  edit { name }
  # Web application firewall configuration.
  set name { string }   WAF Profile name. size[35]
  set external { disable | enable }   Disable/Enable external HTTP Inspection.
  config main-class
    edit { id }
    # Main signature class.
    set id { integer }   Main signature class ID. range[0-4294967295] - datasource(s): waf.main-class.id
    set status { enable | disable }   Status.
    set action { allow | block | erase }   Action.
      allow Allow.
      block Block.
      erase Erase credit card numbers.
    set log { enable | disable }   Enable/disable logging.
    set severity { high | medium | low }   Severity.
      high High severity.
      medium Medium severity.
      low Low severity.
  next
  config disabled-sub-class
    edit { id }
    # Disabled signature subclasses.
    set id { integer }   Signature subclass ID. range[0-4294967295] - datasource(s): waf.sub-class.id
  next
  config disabled-signature
    edit { id }
    # Disabled signatures
    set id { integer }   Signature ID. range[0-4294967295] - datasource(s): waf.signature.id
  next
  set credit-card-detection-threshold { integer }   The minimum number of Credit cards to detect violation. range[0-128]
  config custom-signature
    edit { name }
    # Custom signature.
    set name { string }   Signature name. size[35]
```

```
set status { enable | disable } Status.
set action { allow | block | erase } Action.
    allow Allow.
    block Block.
    erase Erase credit card numbers.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set direction { request | response } Traffic direction.
    request Match HTTP request.
    response Match HTTP response.
set case-sensitivity { disable | enable } Case sensitivity in pattern.
set pattern { string } Match pattern. size[511]
set target { option } Match HTTP target.
    arg HTTP arguments.
    arg-name Names of HTTP arguments.
    req-body HTTP request body.
    req-cookie HTTP request cookies.
    req-cookie-name HTTP request cookie names.
    req-filename HTTP request file name.
    req-header HTTP request headers.
    req-header-name HTTP request header names.
    req-raw-uri Raw URI of HTTP request.
    req-uri URI of HTTP request.
    resp-body HTTP response body.
    resp-hdr HTTP response headers.
    resp-status HTTP response status.

next
set status { enable | disable } Enable/disable the constraint.
set length { integer } Length of HTTP header in bytes (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set length { integer } Length of HTTP content in bytes (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
```

```

        allow Allow.
        block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set length { integer } Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647). range[0-
2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set length { integer } Length of HTTP line in bytes (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set length { integer } Maximum length of URL parameter in bytes (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.

```

```
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set max-cookie { integer } Maximum number of cookies in HTTP request (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set max-header-line { integer } Maximum number HTTP header lines (0 to 2147483647). range[0-2147483647]
```



```
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set max-url-param { integer } Maximum number of parameters in URL (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
set status { enable | disable } Enable/disable the constraint.
set max-range-segment { integer } Maximum number of range segments in HTTP range line (0 to 2147483647). range[0-2147483647]
set action { allow | block } Action.
    allow Allow.
    block Block.
set log { enable | disable } Enable/disable logging.
set severity { high | medium | low } Severity.
    high High severity.
    medium Medium severity.
    low Low severity.
config exception
edit { id }
# HTTP constraint exception.
set id { integer } Exception ID. range[0-4294967295]
set pattern { string } URL pattern. size[511]
set regex { enable | disable } Enable/disable regular expression based pattern match.
set address { string } Host address. size[63] - datasource(s): firewall.address.name, firewall.addrgrp.name
set header-length { enable | disable } HTTP header length in request.
set content-length { enable | disable } HTTP content length in request.
set param-length { enable | disable } Maximum length of parameter in URL, HTTP POST request or HTTP body.
set line-length { enable | disable } HTTP line length in request.
set url-param-length { enable | disable } Maximum length of parameter in URL.
set version { enable | disable } Enable/disable HTTP version check.
set method { enable | disable } Enable/disable HTTP method check.
set hostname { enable | disable } Enable/disable hostname check.
```

```
    set malformed { enable | disable }  Enable/disable malformed HTTP request check.
    set max-cookie { enable | disable }  Maximum number of cookies in HTTP request.
    set max-header-line { enable | disable }  Maximum number of HTTP header line.
    set max-url-param { enable | disable }  Maximum number of parameters in URL.
    set max-range-segment { enable | disable }  Maximum number of range segments in HTTP range line.
  next
set status { enable | disable }  Status.
set log { enable | disable }  Enable/disable logging.
set severity { high | medium | low }  Severity.
    high  High severity
    medium  medium severity
    low  low severity
set default-allowed-methods { option }  Methods.
    get  HTTP GET method.
    post  HTTP POST method.
    put  HTTP PUT method.
    head  HTTP HEAD method.
    connect  HTTP CONNECT method.
    trace  HTTP TRACE method.
    options  HTTP OPTIONS method.
    delete  HTTP DELETE method.
    others  Other HTTP methods.
config method-policy
  edit { id }
  # HTTP method policy.
  set id { integer }  HTTP method policy ID. range[0-4294967295]
  set pattern { string }  URL pattern. size[511]
  set regex { enable | disable }  Enable/disable regular expression based pattern match.
  set address { string }  Host address. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
  set allowed-methods { option }  Allowed Methods.
    get  HTTP GET method.
    post  HTTP POST method.
    put  HTTP PUT method.
    head  HTTP HEAD method.
    connect  HTTP CONNECT method.
    trace  HTTP TRACE method.
    options  HTTP OPTIONS method.
    delete  HTTP DELETE method.
    others  Other HTTP methods.

  next
set status { enable | disable }  Status.
set blocked-log { enable | disable }  Enable/disable logging on blocked addresses.
set severity { high | medium | low }  Severity.
```

```

        high    High severity.
        medium  Medium severity.
        low     Low severity.
config trusted-address
  edit { name }
  # Trusted address.
  set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
config blocked-address
  edit { name }
  # Blocked address.
  set name { string }  Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
  next
config url-access
  edit { id }
  # URL access list
  set id { integer }  URL access ID. range[0-4294967295]
  set address { string }  Host address. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
  set action { bypass | permit | block }  Action.
    bypass  Allow the HTTP request, also bypass further WAF scanning.
    permit  Allow the HTTP request, and continue further WAF scanning.
    block   Block HTTP request.
  set log { enable | disable }  Enable/disable logging.
  set severity { high | medium | low }  Severity.
    high    High severity.
    medium  Medium severity.
    low     Low severity.
config access-pattern
  edit { id }
  # URL access pattern.
  set id { integer }  URL access pattern ID. range[0-4294967295]
  set srcaddr { string }  Source address. size[63] - datasource(s): firewall.address.name,firewall.addrgrp.name
  set pattern { string }  URL pattern. size[511]
  set regex { enable | disable }  Enable/disable regular expression based pattern match.
  set negate { enable | disable }  Enable/disable match negation.
  next
next
set comment { string }  Comment. size[1023]
next
end

```

waf signature

Introduction.

```
config waf signature
  edit { id }
  # Hidden table for datasource.
  set desc { string } Signature description. size[511]
  set id { integer } Signature ID. range[0-4294967295]
  next
end
```

waf sub-class

Introduction.

```
config waf sub-class
  edit { id }
  # Hidden table for datasource.
  set name { string } Signature subclass name. size[127]
  set id { integer } Signature subclass ID. range[0-4294967295]
next
end
```

wanopt

Use these commands to configure FortiGate WAN optimization.

This section includes syntax for the following commands:

- [wanopt auth-group](#)
- [wanopt forticache-service](#)
- [wanopt peer](#)
- [wanopt profile](#)
- [wanopt settings](#)
- [wanopt storage](#)
- [wanopt webcache](#)

wanopt auth-group

Use this command to configure WAN optimization authentication groups, which can be used to support secure tunneling between WAN optimization peers.

```
config wanopt auth-group
  edit { name }
  # Configure WAN optimization authentication groups.
  set name { string } Auth-group name. size[35]
  set auth-method { cert | psk } Select certificate or pre-shared key authentication for this authentication group.
    cert Certificate authentication.
    psk Pre-shared secret key authentication.
  set psk { password_string } Pre-shared key used by the peers in this authentication group. size[128]
  set cert { string } Name of certificate to identify this peer. size[35] - datasource(s): vpn.certificate.local.name
  set peer-accept { any | defined | one } Determine if this auth group accepts, any peer, a list of defined peers, or just one peer.
    any Accept any peer that can authenticate with this auth group.
    defined Accept only the peers added with the wanopt peer command.
    one Accept the peer added to this auth group using the peer option.
  set peer { string } 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. size[35] - datasource(s): wanopt.peer.peer-host-id
  next
end
```

auth-method {cert | psk}

Enter your preferred authentication method:

- Use `cert` (by default) to authenticate using a certificate. Once set, use the `cert` entry to specify the name of the certificate (see below).
- Use `psk` to authenticate using a pre-shared key. Once set, use the `psk` entry to specify the pre-shared key (see below).

cert <name>

Note: This entry is only available when `auth-method` is set to `cert`. Local certificate to be used by the peers in this authentication group. The certificate must have already been installed on the FortiGate before entering it here.

psk <preshared-key>

Note: This entry is only available when `auth-method` is set to `psk`. Pre-shared key to be used for the authentication group.

peer-accept {any | defined | one}

Specify whether the authentication group can be used for `any` peer, only the `defined` peers that have been added to the FortiGate unit, or just `one` specific peer. If you select `one`, use the `peer` entry to add the name of the peer to the authentication group.

peer

Note: This entry is only available when `peer-accept` is set to `one`. Name of one peer to add to this authentication group. The peer must have already been added to the FortiGate before entering it here.

wanopt forticache-service

Use this command to add an external FortiCache service to the FortiGate.

```
config wanopt forticache-service
  set status { disable | enable }  Enable/disable using FortiCache as Web cache storage.
  set local-cache-id { string }  ID that this device uses to connect to the remote FortiCache. size[63]
  set remote-forticache-id { string }  ID of the FortiCache to which the device connects. size[63]
  set remote-forticache-ip { ipv4 address any }  IP address of the FortiCache to which the device connects.
end
```

Supplemental Information

The following section is for those commands that require further explanation.

status {enable | disable}

Enable or disable using FortiCache as a web cache storage. Default is `enable`.

local-cache-id <string>

ID that the FortiGate uses to connect to the remote address of the local FortiCache.

Note: This command is only available if `status` is set to `enable`.

remote-cache-id <string>

ID of the FortiCache to which the FortiGate connects.

Note: This command is only available if `status` is set to `enable`.

remote-forticache-ip <ip_address>

IP address of the FortiCache to which the FortiGate connects.

Note: This command is only available if `status` is set to `enable`.

wanopt peer

Use this command to add WAN optimization peers. This command identifies the other FortiGate units, or peers, that the local FortiGate can form WAN optimization tunnels with. When the remote FortiGate unit connects to the local FortiGate unit to start a WAN optimization tunnel, the remote FortiGate unit local host ID is requested. If the local host ID matches a peer added to the local FortiGate unit, then the local FortiGate unit can accept WAN optimization tunnel from the remote FortiGate unit.

```
config wanopt peer
  edit { peer-host-id }
  # Configure WAN optimization peers.
  set peer-host-id { string } Peer host ID. size[35]
  set ip { ipv4 address any } Peer IP address.
  next
end
```

ip <ipv4-address>

IP address of the interface that the remote FortiGate unit will use to connect to the local FortiGate unit — this is usually the interface connected to the WAN.

wanopt profile

Use this command to configure WAN optimization profiles that work in conjunction with security policies to accept specific traffic. All sessions accepted by a firewall policy, that include a WAN optimization profile, and that match that WAN optimization profile, are processed by WAN optimization. WAN optimization profiles must be added to the FortiGates at each end of the tunnel. To learn more about WAN optimization, including profiles and configuration examples, see [Configuring WAN optimization](#) on our Online Help Portal.

```

config wanopt profile
  edit { name }
    # Configure WAN optimization profiles.
    set name { string } Profile name. size[35]
    set transparent { enable | disable } Enable/disable transparent mode.
    set comments { string } Comment. size[255]
    set auth-group { string } Optionally add an authentication group to restrict access to the WAN Optimization tunnel to peers in the authentication group. size[35] - datasource(s): wanopt.auth-group.name
    set status { enable | disable } Enable/disable HTTP WAN Optimization.
    set secure-tunnel { enable | disable } Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).
    set byte-caching { enable | disable } 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.
    set prefer-chunking { dynamic | fix } Select dynamic or fixed-size data chunking for HTTP WAN Optimization.
      dynamic Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.
      fix Select fixed data chunking.
    set tunnel-sharing { private | shared | express-shared } Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.
      private For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.
      shared For profiles that accept nonaggressive and non-interactive protocols.
      express-shared For profiles that accept interactive protocols such as Telnet.
    set log-traffic { enable | disable } Enable/disable logging.
    set port { integer } 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. range[1-65535]
    set ssl { enable | disable } Enable/disable SSL/TLS offloading (hardware acceleration) for HTTPS traffic in this tunnel.
    set ssl-port { integer } Port on which to expect HTTPS traffic for SSL/TLS offloading. range[1-65535]
    set unknown-http-version { reject | tunnel | best-effort } How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.
      reject Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.
      tunnel 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.

```

    best-effort 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.
    set tunnel-non-http { enable | disable } 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.
    set status { enable | disable } Enable/disable HTTP WAN Optimization.
    set secure-tunnel { enable | disable } Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same
    TCP port (7810).
    set byte-caching { enable | disable } 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.
    set prefer-chunking { dynamic | fix } Select dynamic or fixed-size data chunking for HTTP WAN Optimization.
        dynamic Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown pro-
        tocol.
        fix Select fixed data chunking.
    set tunnel-sharing { private | shared | express-shared } Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-inter-
    active protocols.
        private For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not
        share tunnels with less-aggressive protocols.
        shared For profiles that accept nonaggressive and non-interactive protocols.
        express-shared For profiles that accept interactive protocols such as Telnet.
    set log-traffic { enable | disable } Enable/disable logging.
    set port { integer } 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. range[1-65535]
    set status { enable | disable } Enable/disable HTTP WAN Optimization.
    set secure-tunnel { enable | disable } Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same
    TCP port (7810).
    set byte-caching { enable | disable } 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.
    set tunnel-sharing { private | shared | express-shared } Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-inter-
    active protocols.
        private For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not
        share tunnels with less-aggressive protocols.
        shared For profiles that accept nonaggressive and non-interactive protocols.
        express-shared For profiles that accept interactive protocols such as Telnet.
    set log-traffic { enable | disable } Enable/disable logging.
    set port { integer } 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. range[1-65535]
    set status { enable | disable } Enable/disable HTTP WAN Optimization.
    set secure-tunnel { enable | disable } Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same
    TCP port (7810).
    set byte-caching { enable | disable } 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.
    set prefer-chunking { dynamic | fix } Select dynamic or fixed-size data chunking for HTTP WAN Optimization.

```

```
dynamic Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.
fix Select fixed data chunking.
set tunnel-sharing { private | shared | express-shared } Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.
    private For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.
    shared For profiles that accept nonaggressive and non-interactive protocols.
    express-shared For profiles that accept interactive protocols such as Telnet.
set log-traffic { enable | disable } Enable/disable logging.
set port { integer } 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. range[1-65535]
set status { enable | disable } Enable/disable HTTP WAN Optimization.
set secure-tunnel { enable | disable } Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).
set byte-caching { enable | disable } 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.
set byte-caching-opt { mem-only | mem-disk } Select whether TCP byte-caching uses system memory only or both memory and disk space.
    mem-only Byte caching with memory only.
    mem-disk Byte caching with memory and disk.
set tunnel-sharing { private | shared | express-shared } Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.
    private For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.
    shared For profiles that accept nonaggressive and non-interactive protocols.
    express-shared For profiles that accept interactive protocols such as Telnet.
set log-traffic { enable | disable } Enable/disable logging.
set port { string } 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.
set ssl { enable | disable } Enable/disable SSL/TLS offloading.
set ssl-port { integer } Port on which to expect HTTPS traffic for SSL/TLS offloading. range[1-65535]
next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

transparent {enable | disable}

Enable (by default) or disable transparent mode for this profile. When enabled, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. When disabled, the source address of the packets received by servers is changed to the address of the FortiGate interface, so servers appear to receive packets from the FortiGate. Routing on the server network is simpler in this case because client addresses are not involved, however the server won't be able to tell which individual client is sending traffic.

comments <comments>

Optional comments.

auth-group <group>

Note: Assigning an authentication group is mandatory if `secure-tunnel` has been enabled for the profile. Peer authentication group to be used by this WAN optimization profile. Both client and server FortiGates must add the same authentication group, with both the same names and pre-shared key or certificate.

config {http | cifs | mapi | ftp | tcp}

Use this configuration method to determine various WAN optimization settings for each protocol. The table below depicts those entries that are available for certain protocols (port numbers are the default values for each protocol):

Protocols	http	cifs	mapi	ftp	tcp
byte-caching-opt					✓
prefer-chunking	✓	✓		✓	
port	80	445	135	21	1-65535
ssl	✓				✓

Protocols	http	cifs	mapi	ftp	tcp
ssl-port	443				443 990 995 465 993
unknown-http-version	✓				
tunnel-non-http	✓				

status {enable | disable}

Enable or disable (by default) the profile.

secure-tunnel {enable | disable}

Note: This entry can only be enabled when an authentication group has already been assigned to the profile (see the `auth-group` entry above).

Enable or disable (by default) the use of AES-128bit-CBC SSL to encrypt and secure traffic in the WAN optimization tunnel.

The FortiGates use FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. The secure tunnel uses the same TCP port as a non-secure tunnel (TCP port 7810).

byte-caching {enable | disable}

Enable (by default, *except* `tcp` which is set to `disable`) or disable WAN optimization byte caching for the traffic accepted by this profile.

Byte caching is a WAN optimization technique that reduces the amount of data that has to be transmitted across a WAN by caching file data to be retrieved later, as required.

byte-caching-opt {mem-only | mem-disk}

Note: This entry is only available when configuring `tcp`.

Byte caching method:

- **mem-only:** Byte caching with memory only (set by default).
- **mem-disk:** Byte caching with memory and disk.

prefer-chunking {dynamic | fix}

Note: This entry is only available when configuring either `http`, `cifs`, or `ftp`.

Data chunking preference:

- **dynamic:** Dynamic data chunking preferred. Use to help detect persistent data chunks in a changed file or in an embedded unknown protocol.
- **fix:** Fixed-size data chunking preferred (set by default).

Note that, while `prefer-chunking` is not available in `tcp` or `mapi`, TCP chunking algorithm will be `dynamic`, so long as `byte-caching-opt` is set to `mem-disk`. MAPI only uses `dynamic`, and thus has no option.

tunnel-sharing {private | shared | express-shared}

Tunnel sharing mode:

- **private:** Used for profiles that accept aggressive protocols such as HTTP and FTP so as to not share tunnels with less-aggressive protocols (set by default).
- **shared:** Used for profiles that accept non-aggressive and non-interactive protocols.
- **express-shared:** Used for profiles that accept interactive protocols, such as Telnet.

log-traffic {enable | disable}

Enable (by default) or disable traffic logging.

port <number>

Port used by each protocol for the profile. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this profile.

Set the value between 1-65535 (default values vary between each protocol; see table above).

ssl {enable | disable}

Note: This entry is only available when configuring either `http` or `tcp`.

Enable or disable (by default) SSL offloading for HTTPS traffic.

If enabled, the profile will be ready to accept SSL-encrypted traffic (HTTPS traffic) because `ssl-port` will become available and is set to 443 by default (see entry below). Also, when enabled, you must add an SSL server for each HTTP server that you want to offload SSL encryption/decryption for by using the `config wanopt ssl-server` command.

ssl-port <https-ports>

Note: This entry is only available when `ssl` is set to `enable`.

Ports used for HTTPS traffic offloading. Set value between 1-65535 (default values vary between each protocol; see table above).

unknown-http-version {reject | tunnel | best-effort}

Note: This entry is only available when configuring `http`.

Action to take when an unknown version of HTTP is encountered. Unknown HTTP sessions are those that don't comply with HTTP 0.9, 1.0, or 1.1.

- **reject:** Rejects requests with unknown HTTP version.
- **tunnel:** Tunnels requests with unknown HTTP version (set by default).
- **best-effort:** Proceeds with best effort.

tunnel-non-http {enable | disable}

Note: This entry is only available when configuring `http`.

Enable to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web-caching. TCP protocol optimization is applied to non-HTTP sessions. Disable (by default) to drop non-HTTP sessions that were otherwise accepted by the profile.

wanopt settings

Use this command to enable traffic logging for WAN optimization and WAN optimization web-caching sessions.

```
config wanopt settings
  set host-id { string }   Local host ID (must also be entered in the remote FortiGate's peer list). size[35]
  set tunnel-ssl-algorithm { high | medium | low }   Relative strength of encryption algorithms accepted during tunnel negotiation.
    high   High encryption. Allow only AES and ChaCha.
    medium Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
    low    Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
  set auto-detect-algorithm { simple | diff-req-req }   Auto detection algorithms used in tunnel negotiations.
    simple   Use the same TCP option value in SYN/SYNACK packets. Backward compatible.
    diff-req-req Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.
end
```

host-id <id>

Local host ID/name (set to `default-id` by default). Make sure that the local host ID is also entered in the other FortiGate's peer list.

tunnel-ssl-algorithm {high | medium | low}

Relative strength of encryption accepted for SSL tunnel negotiation:

- **high:** Encryption allows AES and 3DES (set by default).
- **medium:** Encryption allows AES, 3DES, and RC4.
- **low:** Encryption allows AES, 3DES, RC4, and DES.

auto-detect-algorithm {simple | diff-req-req}

Automatic detection algorithms used in tunnel negotiation:

- **simple:** Use the same TCP option value from SYN/SYNACK packets. Backward compatible (set by default).
- **diff-req-req:** Use different TCP option value than in SYN/SYNACK packets to avoid false positive detection.

wanopt storage

Use this command to determine the maximum size of the byte-caching or web-caching database added to the WAN optimization storage. This is determined by setting the total size and then the percentage to be allotted for web-caching. To view the web-cache and WAN optimization cache storage sizes in megabytes instead (and not as a percentage of the total size allotted for the storage), enter the `get` command. The storage sizes will be displayed: `webcache-storage-size` and `wan-optimization-cache-storage-size`. Note that you must have already configured storage settings using the `config system storage` command before you can configure settings here. All FortiGates with hard disks include a default storage name, such as `Internal`.

```
config wanopt storage
  edit { name }
    # Designate logical storage for WAN optimization.
    set name { string } Storage name. size[35] - datasource(s): system.storage.name
    set size { integer } Maximum total size of files in storage (MB), depending on the partition size. range[0-4294967295]
    set webcache-storage-percentage { integer } Percentage of storage available for web-caching (the rest is used for WAN optimization). range
[0-100]
    set webcache-storage-size { string } Web cache storage size.
    set wan-optimization-cache-storage-size { string } WAN optimization cache storage size.
  next
end
```

size <mb>

Maximum total size of files within the storage. Set the value between 512-14518 (or 512MB to just over 14.5GB). The default value depends on the partition size.

webcache-storage-percentage <percentage>

Percentage of storage available for web-caching (the rest is used for WAN optimization). Set the value between 0-100. The default value is set to 50.

wanopt webcache

Use this command to change how the WAN optimization web-cache operates. In most cases the default settings are acceptable, however you may wish to change them to improve performance or optimize the cache for your specific configuration.

```
config wanopt webcache
  set max-object-size { integer } 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. range[1-2147483]
  set neg-resp-time { integer } Time in minutes to cache negative responses or errors (0 - 4294967295, default = 0 which means negative responses are not cached). range[0-4294967295]
  set fresh-factor { integer } 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. range[1-100]
  set max-ttl { integer } 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 (100 years)). range[1-5256000]
  set min-ttl { integer } 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 (100 years)). range[1-5256000]
  set default-ttl { integer } Default object expiry time (default = 1440 min (1 day); maximum = 5256000 min (100 years)). This only applies to those objects that do not have an expiry time set by the web server. range[1-5256000]
  set ignore-ims { enable | disable } Enable/disable ignoring the if-modified-since (IMS) header.
  set ignore-conditional { enable | disable } Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.
  set ignore-pnc { enable | disable } Enable/disable ignoring the pragma no-cache (PNC) header.
  set ignore-ie-reload { enable | disable } Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.
  set cache-expired { enable | disable } Enable/disable caching type-1 objects that are already expired on arrival.
  set cache-cookie { enable | disable } Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached..
  set reval-pnc { enable | disable } Enable/disable revalidation of pragma-no-cache (PNC) to address bandwidth concerns.
  set always-revalidate { enable | disable } Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.
  set cache-by-default { enable | disable } Enable/disable caching content that lacks explicit caching policies from the server.
  set host-validate { enable | disable } Enable/disable validating "Host:" with original server IP.
  set external { enable | disable } Enable/disable external Web caching.
end
```

Supplemental Information

The following section is for those commands that require further explanation.

max-object-size <kb>

Maximum cacheable object size in kB. All objects retrieved that are larger than the maximum size are delivered to the client but are not stored in the web cache. Set value between 1-2147483 (or 1kB to just over 2GB). The default value is set to 512000 (or 512MB).

neg-resp-time <minutes>

Period of time in minutes to cache negative responses. The default value is set to 0, meaning no negative responses will be cached.

fresh-factor <percentage>

The fresh factor as a percentage. For cached objects that don't have an expiry time, the web cache periodically checks the server to see if any objects have expired. The higher the fresh factor, the less often the checks occur. Set the value between 0-100. The default value is set to 100.

max-ttl

Maximum time-to-live period in minutes an object can stay in the web cache without checking to see if it has expired on the server. Set the value between 1-5256000. The default value is set to 7200 (or five days).

min-ttl

Minimum time-to-live period in minutes an object can stay in the web cache without checking to see if it has expired on the server. Set the value between 1-5256000. The default value is set to 5.

default-ttl

The default period of time in minutes before an object expires. This only applies to those objects that do not already have an expiry time set by the web server. Set the value between 1-5256000. The default value is set to 1440 (or one day).

ignore-ims {enable | disable}

Enable or disable (by default) the if-modified-since (IMS) header to be ignored. If the time specified by the IMS header in the client's conditional request is greater than the last modified time of the object in the cache, it is likely that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object. Enabling `ignore-ims` overrides this behaviour.

ignore-conditional {enable | disable}

Enable or disable (by default) controlling the behaviour of cache-control header values. HTTP 1.1 provides additional controls to the client over the behaviour of caches concerning the staleness of the object. Depending on various Cache-Control headers, the FortiGate can be forced to consult the OCS before serving the object from the cache. For more information about the behaviour of cache-control header values, see [RFC 2616](#).

ignore-pnc {enable | disable}

Enable or disable (by default) the pragma no-cache (PNC) header to be ignored. Typically, if a client sends an HTTP GET request with a PNC header, a cache must consult the OCS before serving the content. This means the FortiGate always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this, PNC requests can degrade performance and increase server-side bandwidth. Enabling `ignore-pnc` ignores the PNC header from the client request.

ignore-ie-reload {enable | disable}

Enable (by default) or disable the FortiGate to ignore the PNC interpretation of Internet Explorer's Accept: / header. Some versions of Internet Explorer issue Accept: / headers instead of PNC headers when you select **Refresh**. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object. Enabling `ignore-ie-reload` ignores this interpretation.

cache-expired {enable | disable}

Enable or disable (by default) caching of type-1 objects that are already expired upon acquisition. When this setting is enabled, type-1 objects that are already expired at the time of acquisition are cached (if all other conditions make the object cachable). If disabled, expired type-1 objects are considered non-cachable.

cache-cookie {enable | disable}

Enable or disable (by default) the caching of cookies. Typically, it is best to not perform cookie caching, as HTTP responses with cookies contain specific user data.

reval-pnc {enable | disable}

Enable or disable (by default) PNC revalidation to address bandwidth concerns. The PNC header in a client's request can affect the efficiency of the FortiGate unit from a bandwidth gain perspective. If you do not want to completely ignore PNC in client requests (such as when using the `ignore-pnc` entry shown above), you can lower the impact of the PNC by enabling `reval-pnc`.

always-revalidate {enable | disable}

Enable or disable (by default) the revalidation of requested cached objects, which have content on the server, before serving it to the client.

cache-by-default {enable | disable}

Enable or disable (by default) the caching of content that lack explicit caching policies from the server.

host-validate {enable | disable}

Enable or disable (by default) the validation of Host: header with original server IP.

external {enable | disable}

Enable or disable (by default) external cache.

webfilter

Introduction.

This section includes syntax for the following commands:

- `webfilter content`
- `webfilter content-header`
- `webfilter cookie-ovrd`
- `webfilter fortiguard`
- `webfilter ftgd-local-cat`
- `webfilter ftgd-local-rating`
- `webfilter ips-urlfilter-cache-setting`
- `webfilter ips-urlfilter-setting`
- `webfilter override`
- `webfilter profile`
- `webfilter search-engine`
- `webfilter urlfilter`

webfilter content

Introduction.

```
config webfilter content
  edit { id }
  # Configure Web filter banned word table.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
  edit { name }
  # Configure banned word entries.
  set name { string } Banned word. size[127]
  set pattern-type { wildcard | regexp } Banned word pattern type: wildcard pattern or Perl regular expression.
    wildcard Wildcard pattern.
    regexp Perl regular expression.
  set status { enable | disable } Enable/disable banned word.
  set lang { option } Language of banned word.
    western Western.
    simch Simplified Chinese.
    trach Traditional Chinese.
    japanese Japanese.
    korean Korean.
    french French.
    thai Thai.
    spanish Spanish.
    cyrillic Cyrillic.
  set score { integer } Score, to be applied every time the word appears on a web page (0 - 4294967295, default = 10). range[0-4294967295]
  set action { block | exempt } Block or exempt word when a match is found.
    block Block matches.
    exempt Exempt matches.
  next
next
end
```

webfilter content-header

Introduction.

```
config webfilter content-header
  edit { id }
  # Configure content types used by Web filter.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of table. size[35]
  set comment { string } Optional comments. size[255]
  config entries
    edit { pattern }
    # Configure content types used by web filter.
    set pattern { string } Content type (regular expression). size[31]
    set action { block | allow | exempt } Action to take for this content type.
      block Block content type.
      allow Allow content type.
      exempt Exempt content type.
    set category { string } Categories that this content type applies to.
  next
next
end
```

webfilter cookie-ovrd

Introduction.

```
config webfilter cookie-ovrd
  set redir-host { string } Domain name or IP of host that will be used to validate override authentication cookies. size[255]
  set redir-port { integer } TCP port that will be used on "redir-host" to validate override authentication cookies. range[0-65535]
end
```

webfilter fortiguard

Introduction.

```
config webfilter fortiguard
  set cache-mode { ttl | db-ver }  Cache entry expiration mode.
    ttl      Expire cache items by time-to-live.
    db-ver   Expire cache items when the server DB version changes.
  set cache-prefix-match { enable | disable }  Enable/disable prefix matching in the cache.
  set cache-mem-percent { integer }  Maximum percentage of available memory allocated to caching (1 - 15%). range[1-15]
  set ovr-auth-port-http { integer }  Port to use for FortiGuard Web Filter HTTP override authentication range[0-65535]
  set ovr-auth-port-https { integer }  Port to use for FortiGuard Web Filter HTTPS override authentication. range[0-65535]
  set ovr-auth-port-warning { integer }  Port to use for FortiGuard Web Filter Warning override authentication. range[0-65535]
  set ovr-auth-https { enable | disable }  Enable/disable use of HTTPS for override authentication.
  set warn-auth-https { enable | disable }  Enable/disable use of HTTPS for warning and authentication.
  set close-ports { enable | disable }  Close ports used for HTTP/HTTPS override authentication and disable user overrides.
  set request-packet-size-limit { integer }  Limit size of URL request packets sent to FortiGuard server (0 for default). range[576-10000]
  set ovr-auth-port { integer }  Port to use for FortiGuard Web Filter override authentication. range[0-65535]
end
```

webfilter ftgd-local-cat

Introduction.

```
config webfilter ftgd-local-cat
  edit { desc }
  # Configure FortiGuard Web Filter local categories.
  set id { integer } Local category ID. range[140-191]
  set desc { string } Local category description. size[79]
  next
end
```

webfilter ftgd-local-rating

Introduction.

```
config webfilter ftgd-local-rating
  edit { url }
  # Configure local FortiGuard Web Filter local ratings.
  set url { string } URL to rate locally. size[511]
  set status { enable | disable } Enable/disable local rating.
  set rating { string } Local rating.
next
end
```

webfilter ips-urlfilter-cache-setting

Introduction.

```
config webfilter ips-urlfilter-cache-setting
    set dns-retry-interval { integer }    Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL
only. range[0-2147483]
    set extended-ttl { integer }    Extend time to live beyond reported by DNS. 0 means use DNS server's TTL range[0-2147483]
end
```

webfilter ips-urlfilter-setting

Introduction.

```
config webfilter ips-urlfilter-setting
  set device { string } Enable/disable gateway out interface. size[35] - datasource(s): system.interface.name
  set distance { integer } Administrative distance (1 - 255). range[1-255]
  set gateway { ipv4 address } Gateway IP for this route.
end
```


webfilter override

Introduction.

```
config webfilter override
  edit { id }
  # Configure FortiGuard Web Filter administrative overrides.
  set id { integer }  Override rule ID. range[0-4294967295]
  set status { enable | disable }  Enable/disable override rule.
  set scope { user | user-group | ip | ip6 }  Override either the specific user, user group, IPv4 address, or IPv6 address.
    user      Override the specified user.
    user-group  Override the specified user group.
    ip        Override the specified IP address.
    ip6       Override the specified IPv6 address.
  set ip { ipv4 address }  IPv4 address which the override applies.
  set user { string }  Name of the user which the override applies. size[64]
  set user-group { string }  Specify the user group for which the override applies. size[63] - datasource(s): user.group.name
  set old-profile { string }  Name of the web filter profile which the override applies. size[35] - datasource(s): webfilter.profile.name
  set new-profile { string }  Name of the new web filter profile used by the override. size[35] - datasource(s): webfilter.profile.name
  set ip6 { ipv6 address }  IPv6 address which the override applies.
  set expires { string }  Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).
  set initiator { string }  Initiating user of override (read-only setting). size[64]
next
end
```

webfilter profile

Introduction.

```

config webfilter profile
  edit { name }
  # Configure Web filter profiles.
  set name { string } Profile name. size[35]
  set comment { string } Optional comments. size[255]
  set replacemsg-group { string } Replacement message group. size[35] - datasource(s): system.replacemsg-group.name
  set inspection-mode { proxy | flow-based } Web filtering inspection mode.
    proxy Proxy.
    flow-based Flow based.
  set options { option } Options.
    activexfilter ActiveX filter.
    cookiefilter Cookie filter.
    javafilter Java applet filter.
    block-invalid-url Block sessions contained an invalid domain name.
    jscript Javascript block.
    js JS block.
    vbs VB script block.
    unknown Unknown script block.
    intrinsic Intrinsic script block.
    wf-referer Referring block.
    wf-cookie Cookie block.
    per-user-bwl Per-user black/white list filter
  set https-replacemsg { enable | disable } Enable replacement messages for HTTPS.
  set ovr-d-perm { bannedword-override | urlfilter-override | fortiguard-wf-override | contenttype-check-override } Permitted override types.
    bannedword-override Banned word override.
    urlfilter-override URL filter override.
    fortiguard-wf-override FortiGuard Web Filter override.
    contenttype-check-override Content-type header override.
  set post-action { normal | block } Action taken for HTTP POST traffic.
    normal Normal, POST requests are allowed.
    block POST requests are blocked.
  set ovr-d-cookie { allow | deny } Allow/deny browser-based (cookie) overrides.
    allow Allow browser-based (cookie) override.
    deny Deny browser-based (cookie) override.
  set ovr-d-scope { option } Override scope.

```

```

    user          Override for the user.
    user-group    Override for the user's group.
    ip            Override for the initiating IP.
    browser       Create browser-based (cookie) override.
    ask           Prompt for scope when initiating an override.
set profile-type { list | radius }  Override profile type.
    list         Profile chosen from list.
    radius       Profile determined by RADIUS server.
set ovrd-dur-mode { constant | ask }  Override duration mode.
    constant     Constant mode.
    ask          Prompt for duration when initiating an override.
set ovrd-dur { string }  Override duration.
set profile-attribute { option }  Profile attribute to retrieve from the RADIUS server.
    User-Name          Use this attribute.
    User-Password      Use this attribute.
    CHAP-Password      Use this attribute.
    NAS-IP-Address     Use this attribute.
    NAS-Port           Use this attribute.
    Service-Type       Use this attribute.
    Framed-Protocol    Use this attribute.
    Framed-IP-Address  Use this attribute.
    Framed-IP-Netmask  Use this attribute.
    Framed-Routing     Use this attribute.
    Filter-Id          Use this attribute.
    Framed-MTU         Use this attribute.
    Framed-Compression Use this attribute.
    Login-IP-Host      Use this attribute.
    Login-Service      Use this attribute.
    Login-TCP-Port     Use this attribute.
    Reply-Message      Use this attribute.
    Callback-Number    Use this attribute.
    Callback-Id        Use this attribute.
    Framed-Route       Use this attribute.
    Framed-IPX-Network Use this attribute.
    State              Use this attribute.
    Class              Use this attribute.
    Session-Timeout    Use this attribute.
    Idle-Timeout       Use this attribute.
    Termination-Action Use this attribute.
    Called-Station-Id  Use this attribute.
    Calling-Station-Id Use this attribute.
    NAS-Identifier     Use this attribute.
    Proxy-State        Use this attribute.

```

```

Login-LAT-Service      Use this attribute.
Login-LAT-Node        Use this attribute.
Login-LAT-Group       Use this attribute.
Framed-AppleTalk-Link Use this attribute.
Framed-AppleTalk-Network Use this attribute.
Framed-AppleTalk-Zone Use this attribute.
Acct-Status-Type     Use this attribute.
Acct-Delay-Time      Use this attribute.
Acct-Input-Octets    Use this attribute.
Acct-Output-Octets   Use this attribute.
Acct-Session-Id     Use this attribute.
Acct-Authentic       Use this attribute.
Acct-Session-Time    Use this attribute.
Acct-Input-Packets   Use this attribute.
Acct-Output-Packets  Use this attribute.
Acct-Terminate-Cause Use this attribute.
Acct-Multi-Session-Id Use this attribute.
Acct-Link-Count      Use this attribute.
CHAP-Challenge       Use this attribute.
NAS-Port-Type        Use this attribute.
Port-Limit           Use this attribute.
Login-LAT-Port       Use this attribute.
config ovrdr-user-group
  edit { name }
  # User groups with permission to use the override.
  set name { string } User group name. size[64] - datasource(s): user.group.name
  next
config profile
  edit { name }
  # Web filter profile with permission to create overrides.
  set name { string } Web profile. size[64] - datasource(s): webfilter.profile.name
  next
set bword-threshold { integer } Banned word score threshold. range[0-2147483647]
set bword-table { integer } Banned word table ID. range[0-4294967295] - datasource(s): webfilter.content.id
set urlfilter-table { integer } URL filter table ID. range[0-4294967295] - datasource(s): webfilter.urlfilter.id
set content-header-list { integer } Content header list. range[0-4294967295] - datasource(s): webfilter.content-header.id
set blacklist { enable | disable } Enable/disable automatic addition of URLs detected by FortiSandbox to blacklist.
set whitelist { option } FortiGuard whitelist settings.
  exempt-av           Exempt antivirus.
  exempt-webcontent   Exempt web content.
  exempt-activex-java-cookie Exempt ActiveX-JAVA-Cookie.
  exempt-dlp          Exempt DLP.
  exempt-rangeblock   Exempt RangeBlock.

```

```

        extended-log-others      Support extended log.
set safe-search { url | header } Safe search type.
    url      Insert safe search string into URL.
    header   Insert safe search header.
set youtube-restrict { none | strict | moderate } YouTube EDU filter level.
    none     Full access for YouTube.
    strict   Strict access for YouTube.
    moderate Moderate access for YouTube.
set log-search { enable | disable } Enable/disable logging all search phrases.
config keyword-match
    edit { pattern }
        # Search keywords to log when match is found.
        set pattern { string } Pattern/keyword to search for. size[64]
    next
set options { option } Options for FortiGuard Web Filter.
    error-allow      Allow web pages with a rating error to pass through.
    http-err-detail  Display a replacement message for blocked 4xx and 5xx HTTP errors.
    rate-server-ip   Rate the server IP in addition to the domain name.
    connect-request-bypass Bypass connection which has CONNECT request.
    ftgd-disable     Disable FortiGuard scanning.
set category-override { string } Local categories take precedence over FortiGuard categories.
set exempt-quota { string } Do not stop quota for these categories.
set ovr { string } Allow web filter profile overrides.
config filters
    edit { id }
        # FortiGuard filters.
        set id { integer } ID number. range[0-255]
        set category { integer } Categories and groups the filter examines. range[0-255]
        set action { block | authenticate | monitor | warning } Action to take for matches.
            block      Block access.
            authenticate Authenticate user before allowing access.
            monitor     Allow access while logging the action.
            warning     Allow access after warning the user.
        set warn-duration { string } Duration of warnings.
    config auth-usr-grp
        edit { name }
            # Groups with permission to authenticate.
            set name { string } User group name. size[64] - datasource(s): user.group.name
        next
    set log { enable | disable } Enable/disable logging.
    set override-replacemsg { string } Override replacement message. size[28]
    set warning-prompt { per-domain | per-category } Warning prompts in each category or each domain.
        per-domain    Per-domain warnings.

```

```

        per-category Per-category warnings.
    set warning-duration-type { session | timeout } Re-display warning after closing browser or after a timeout.
        session After session ends.
        timeout After timeout occurs.

    next
config quota
    edit { id }
    # FortiGuard traffic quota settings.
    set id { integer } ID number. range[0-4294967295]
    set category { string } FortiGuard categories to apply quota to (category action must be set to monitor).
    set type { time | traffic } Quota type.
        time Use a time-based quota.
        traffic Use a traffic-based quota.
    set unit { B | KB | MB | GB } Traffic quota unit of measurement.
        B Quota in bytes.
        KB Quota in kilobytes.
        MB Quota in megabytes.
        GB Quota in gigabytes.
    set value { integer } Traffic quota value. range[1-4294967295]
    set duration { string } Duration of quota.
    set override-replacemsg { string } Override replacement message. size[28]

    next
set max-quota-timeout { integer } Maximum FortiGuard quota used by single page view in seconds (excludes streams). range[1-86400]
set rate-image-urls { disable | enable } Enable/disable rating images by URL.
set rate-javascript-urls { disable | enable } Enable/disable rating JavaScript by URL.
set rate-css-urls { disable | enable } Enable/disable rating CSS by URL.
set rate-crl-urls { disable | enable } Enable/disable rating CRL by URL.
set wisp { enable | disable } Enable/disable web proxy WISP.
config wisp-servers
    edit { name }
    # WISP servers.
    set name { string } Server name. size[64] - datasource(s): web-proxy.wisp.name

    next
set wisp-algorithm { primary-secondary | round-robin | auto-learning } WISP server selection algorithm.
    primary-secondary Select the first healthy server in order.
    round-robin Select the next healthy server.
    auto-learning Select the lightest loading healthy server.
set log-all-url { enable | disable } Enable/disable logging all URLs visited.
set web-content-log { enable | disable } Enable/disable logging logging blocked web content.
set web-filter-activex-log { enable | disable } Enable/disable logging logging ActiveX.
set web-filter-command-block-log { enable | disable } Enable/disable logging logging blocked commands.
set web-filter-cookie-log { enable | disable } Enable/disable logging logging cookie filtering.
set web-filter-applet-log { enable | disable } Enable/disable logging logging Java applets.

```

```
set web-filter-jscript-log { enable | disable } Enable/disable logging JScripts.
set web-filter-js-log { enable | disable } Enable/disable logging Java scripts.
set web-filter-vbs-log { enable | disable } Enable/disable logging VBS scripts.
set web-filter-unknown-log { enable | disable } Enable/disable logging unknown scripts.
set web-filter-referer-log { enable | disable } Enable/disable logging referrers.
set web-filter-cookie-removal-log { enable | disable } Enable/disable logging blocked cookies.
set web-url-log { enable | disable } Enable/disable logging URL filtering.
set web-invalid-domain-log { enable | disable } Enable/disable logging invalid domain names.
set web-ftgd-err-log { enable | disable } Enable/disable logging rating errors.
set web-ftgd-quota-usage { enable | disable } Enable/disable logging daily quota usage.
next
end
```

webfilter search-engine

Introduction.

```
config webfilter search-engine
  edit { name }
  # Configure web filter search engines.
  set name { string } Search engine name. size[35]
  set hostname { string } Hostname (regular expression). size[127]
  set url { string } URL (regular expression). size[127]
  set query { string } Code used to prefix a query (must end with an equals character). size[15]
  set safesearch { disable | url | header } Safe search method. You can disable safe search, add the safe search string to URLs, or insert a
safe search header.
    disable Site does not support safe search.
    url Safe search selected with a parameter in the URL.
    header Safe search selected by search header (i.e. youtube.edu).
  set charset { utf-8 | gb2312 } Search engine charset.
    utf-8 UTF-8 encoding.
    gb2312 GB2312 encoding.
  set safesearch-str { string } Safe search parameter used in the URL. size[79]
  next
end
```


webfilter urlfilter

Introduction.

```

config webfilter urlfilter
  edit { id }
  # Configure URL filter lists.
  set id { integer } ID. range[0-4294967295]
  set name { string } Name of URL filter list. size[35]
  set comment { string } Optional comments. size[255]
  set one-arm-ips-urlfilter { enable | disable } Enable/disable DNS resolver for one-arm IPS URL filter operation.
  set ip-addr-block { enable | disable } Enable/disable blocking URLs when the hostname appears as an IP address.
config entries
  edit { id }
  # URL filter entries.
  set id { integer } Id. range[0-4294967295]
  set url { string } URL to be filtered. size[511]
  set type { simple | regex | wildcard } Filter type (simple, regex, or wildcard).
    simple Simple URL string.
    regex Regular expression URL string.
    wildcard Wildcard URL string.
  set action { exempt | block | allow | monitor } Action to take for URL filter matches.
    exempt Exempt matches.
    block Block matches.
    allow Allow matches (no log).
    monitor Allow matches (with log).
  set status { enable | disable } Enable/disable this URL filter.
  set exempt { option } If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple
options with a space.
    av AntiVirus scanning.
    web-content Web filter content matching.
    activex-java-cookie ActiveX, Java, and cookie filtering.
    dlp DLP scanning.
    fortiguard FortiGuard web filtering.
    range-block Range block feature.
    pass Pass single connection from all.
    all Exempt from all security profiles.
  set web-proxy-profile { string } Web proxy profile. size[63] - datasource(s): web-proxy.profile.name
  set referrer-host { string } Referrer host name. size[255]

```

```
    next
  next
end
```

web-proxy

Use these commands to configure the FortiGate web proxy. You can use the FortiGate web proxy and interface settings to enable explicit HTTP and HTTPS proxying on one or more interfaces. When enabled, the FortiGate unit becomes a web proxy server. All HTTP and HTTPS session received by interfaces with explicit web proxy enabled are intercepted by the explicit web proxy relayed to their destinations.

To use the explicit proxy, users must add the IP address of a FortiGate interface and the explicit proxy port number to the proxy configuration settings of their web browsers.

This section includes syntax for the following commands:

- [web-proxy debug-url](#)
- [web-proxy explicit](#)
- [web-proxy forward-server](#)
- [web-proxy forward-server-group](#)
- [web-proxy global](#)
- [web-proxy profile](#)
- [web-proxy url-match](#)
- [web-proxy wisp](#)

web-proxy debug-url

Use this command to configure debug URL addresses.

```
config web-proxy debug-url
  edit { name }
  # Configure debug URL addresses.
  set name { string }   Debug URL name. size[63]
  set url-pattern { string }   URL exemption pattern. size[511]
  set status { enable | disable }   Enable/disable this URL exemption.
  set exact { enable | disable }   Enable/disable matching the exact path.
  next
end
```

url-pattern <string>

URL exemption pattern.

status {enable | disable}

Enable (by default) or disable this URL exemption.

exact {enable | disable}

Enable (by default) or disable match exact path.

web-proxy explicit

Note: This command is only available when the FortiGate is in Proxy-based inspection mode.

Use this command to enable the explicit web proxy and the TCP port used by the explicit proxy.

To avoid repetition, only the following entries are available to begin with until `status` is set to `enable`:

- `status`
- `ipv6-status`
- `strict-guest`
- `https-replacement-message`
- `ssl-algorithm`

```
config web-proxy explicit
  set status { enable | disable }  Enable/disable the explicit Web proxy for HTTP and HTTPS session.
  set ftp-over-http { enable | disable }  Enable to proxy FTP-over-HTTP sessions sent from a web browser.
  set socks { enable | disable }  Enable/disable the SOCKS proxy.
  set http-incoming-port { string }  Accept incoming HTTP requests on one or more ports (0 - 65535, default = 8080).
  set https-incoming-port { string }  Accept incoming HTTPS requests on one or more ports (0 - 65535, default = 0, use the same as HTTP).
  set ftp-incoming-port { string }  Accept incoming FTP-over-HTTP requests on one or more ports (0 - 65535, default = 0; use the same as HTTP).
  set socks-incoming-port { string }  Accept incoming SOCKS proxy requests on one or more ports (0 - 65535, default = 0; use the same as HTTP).
  set incoming-ip { ipv4 address any }  Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.
  set outgoing-ip { ipv4 address any }  Outgoing HTTP requests will have this IP address as their source address. An interface must have this IP address.
  set ipv6-status { enable | disable }  Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.
  set incoming-ip6 { ipv6 address }  Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.
  set outgoing-ip6 { ipv6 address }  Outgoing HTTP requests will leave this IPv6. Multiple interfaces can be specified. Interfaces must have these IPv6 addresses.
  set strict-guest { enable | disable }  Enable/disable strict guest user checking by the explicit web proxy.
  set pref-dns-result { ipv4 | ipv6 }  Prefer resolving addresses using the configured IPv4 or IPv6 DNS server (default = ipv4).
    ipv4  Prefer the IPv4 DNS server.
    ipv6  Prefer the IPv6 DNS server.
  set unknown-http-version { reject | best-effort }  Either reject unknown HTTP traffic as malformed or handle unknown HTTP traffic as best as the proxy server can.
```

```

    reject      Reject requests with an unknown HTTP version.
    best-effort Accept requests with an unknown HTTP version and use best efforts to handle the session.
set realm { string } Authentication realm used to identify the explicit web proxy (maximum of 63 characters). size[63]
set sec-default-action { accept | deny } Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.
    accept      Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.
    deny       Deny requests unless there is a matching explicit web proxy policy.
set https-replacement-message { enable | disable } Enable/disable sending the client a replacement message for HTTPS requests.
set message-upon-server-error { enable | disable } Enable/disable displaying a replacement message when a server error is detected.
set pac-file-server-status { enable | disable } Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.
set pac-file-server-port { string } 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).
set pac-file-name { string } Name of the PAC file (default = proxy.pac) size[63]
set pac-file-data { string } PAC file contents enclosed in quotes (maximum of 8192 bytes).
set pac-file-url { string } PAC file access URL.
set ssl-algorithm { high | medium | low } Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.
    high       High encryption. Allow only AES and ChaCha.
    medium     Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
    low        Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
set trace-auth-no-rsp { enable | disable } Enable/disable logging timed-out authentication requests.
end

```

Supplemental Information

The following section is for those commands that require further explanation.

append {outgoing-ip | outgoing-ip6} <ip-addresses>

Note: This entry is *not* available in Transparent mode.

Append IP addresses (IPv4 or IPv6) that outgoing HTTP requests will leave through. Note that an interface must have this IP address to be configured here.

status {enable | disable}

Enable or disable (by default) the explicit web proxy for HTTP and HTTPS sessions.

ftp-over-http {enable | disable}

Enable or disable (by default) ability to proxy FTP sessions sent from a web browser. Once enabled, use the `ftp-incoming-port` entry to set the port that FTP-over-HTTP requests will be accepted on. Note that the explicit proxy only supports FTP with a web browser, not with a standalone FTP client.

socks {enable | disable}

Enable or disable (by default) the Socket Secure (SOCKS) proxy. Once enabled, use the `socks-incoming-port` entry to set the port number that SOCKS traffic from client web browsers will use to connect to the explicit proxy.

http-incoming-port <port>

Port number that HTTP traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 8080. Note that explicit proxy users must configure their web browser's HTTP proxy settings to use this port.

https-incoming-port <port>

Port number that HTTPS traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP. Note that explicit proxy users must configure their web browser's HTTPS proxy settings to use this port.

ftp-incoming-port <port>

Note: This entry is only available when `ftp-over-http` is set to `enable`.

Port number that FTP-over-HTTP traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to . Port number that FTP-over-HTTP traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP. Note that explicit proxy users must configure their web browser's FTP proxy settings to use this port.

socks-incoming-port <port>

Note: This entry is only available when `socks` is set to `enable`.

Port number that SOCKS traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP.

{incoming-ip | incoming-ip6} <ip-addresses>

Note: This entry is *not* available in Transparent mode.

IP address (IPv4 or IPv6) of a FortiGate interface that should accept sessions for the explicit web proxy. Use this command to restrict the explicit web proxy to only accepting sessions from one FortiGate interface. The destination IP address of explicit web proxy sessions should match this IP address.

{outgoing-ip | outgoing-ip6} <ip-addresses>

Note: This entry is *not* available in Transparent mode. IP addresses (IPv4 or IPv6) that outgoing HTTP requests will leave through. Note that an interface must have this IP address to be configured here. Multiple interfaces can be specified. This IP address becomes the source address of web proxy sessions exiting the FortiGate.

ipv6-status {enable | disable}

Enable or disable (by default) IPv6 web proxy functionality. Note that all entries in this command involving IPv6 are only available when `ipv6-status` is set to `enable`.

strict-guest {enable | disable}

Enable or disable (by default) strict guest user check in explicit proxy.

unknown-http-version {reject | best-effort}

Action to take when the proxy server handles an unknown HTTP version request or message:

- **reject:** Treats the HTTP traffic as malformed and drops it (set by default; more secure option).
 - **best-effort:** Attempts to handle the HTTP traffic as best as it can.
-

realm <name>

Name of the authentication realm used to identify the explicit web proxy. Text string can be up to a maximum of 63 characters. If the realm's name includes spaces, enclose it in quotes. No special characters are permitted; only use alphanumeric characters. When a user authenticates with the explicit proxy the

HTTP authentication dialog includes the realm so users can use the realm to identify the explicit web proxy.

sec-default-action {accept | deny}

Determines whether the explicit web proxy accepts or denies (by default) sessions if firewall policies have *not* been added for the explicit web proxy.

https-replacement-message {enable | disable}

Enable (by default) or disable the return of a replacement message for HTTPS requests.

message-upon-server-error {enable | disable}

Enable (by default) or disable the return of a replacement message upon server error detection.

pac-file-server-status {enable | disable}

Enable or disable (by default) Proxy Auto-Configuration (PAC) file server settings.

pac-file-server-port <port>

Note: This entry is only available when `pac-file-server-status` is set to `enable`.

Port number that PAC traffic from client web browsers will use to connect to the explicit proxy. Set the value between 0-65535. The default is set to 0, meaning it will use the same port as HTTP. Note that explicit proxy users must configure their web browser's PAC proxy settings to use this port.

pac-file-name <name>

Note: This entry is only available when `pac-file-server-status` is set to `enable`.

Name of the PAC file. The default is set to `proxy.pac`.

pac-file-data <file>

Note: This entry is only available when `pac-file-server-status` is set to `enable`.

Contents of the PAC file made available from the explicit proxy server for PAC support. Enclose the PAC file text in quotes. The maximum PAC file size is 8192 bytes. You can also copy the contents of a PAC text file and paste the contents into the CLI, so long as the pasted content is between two quotation marks. You can use any PAC file syntax that is supported by your users's browsers. The FortiGate does not parse the PAC file.

pac-file-url <url>

Note: This entry is only available to read when you enter `get`; you *cannot* use this entry to edit the PAC file URL. The PAC file URL is made up of the values entered in both `pac-file-server-port` and `pac-file-name` entries.

Displays the PAC file URL in the following format:

```
http://<interface-ip>:<pac-port>/<pac-name>
```

By default, `<pac-port>` references the value entered in the `http-incoming-port` entry (see above). However, it will instead reference the value entered in `pac-file-server-port` *if* it is changed from its default value. The `<interface-ip>` component of the URL is the interface of the explicit web proxy.

If the explicit web proxy is enabled on multiple interfaces there will be multiple PAC URLs. If you have configured an `incoming-ip` (see entry above) then only one PAC file URL is listed. This URL is to be distributed to PAC users.

ssl-algorithm {high | medium | low}

Relative strength of encryption accepted for deep scan:

- **high:** Encryption allows AES and 3DES.
- **medium:** Encryption allows AES, 3DES, and RC4.
- **low:** Encryption allows AES, 3DES, RC4, and DES (set by default).

trace-auth-rsp {enable | disable}

Enable or disable (by default) tracing (or logging) of timed-out authentication requests.

web-proxy forward-server

Use this command to support explicit web proxy forwarding, also known as proxy chaining.

```
config web-proxy forward-server
edit { name }
# Configure forward-server addresses.
set name { string } Server name. size[63]
set addr-type { ip | fqdn } Address type of the forwarding proxy server: IP or FQDN.
    ip Use an IP address for the forwarding proxy server.
    fqdn Use the FQDN for the forwarding proxy server.
set ip { ipv4 address any } Forward proxy server IP address.
set fqdn { string } Forward server Fully Qualified Domain Name (FQDN). size[255]
set port { integer } Port number that the forwarding server expects to receive HTTP sessions on (1 - 65535, default = 3128). range[1-65535]
set healthcheck { disable | enable } 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.
set monitor { string } URL for forward server health check monitoring (default = http://www.google.com). size[255]
set server-down-option { block | pass } 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.
    block Block sessions until the server is back up.
    pass Pass sessions to their destination bypassing the forward server.
set comment { string } Comment. size[63]
next
end
```

ip <ipv4-address>

Note: This entry is only available when `addr-type` is set to `ip`. IP address of the forwarding proxy server.

fqdn <fqdn>

Note: This entry is only available when `addr-type` is set to `fqdn`. Fully Qualified Domain Name (FQDN) of the forwarding proxy server.

addr-type {ip | fqdn}

Address type of the forwarding proxy server: IP (by default) or FQDN.

port <port>

Port number that the forwarding server expects to receive HTTP sessions on. Set the value between 1-65535. The default is set to 3128.

healthcheck {enable | disable}

Enable or disable (by default) proxy server health check, a function that attempts to connect to a web server to make sure that the remote forwarding server is operating. Once enabled, use the `monitor` entry to set the forward health checking URL.

monitor <url>

Note: This entry is only available when `health-check` is set to `enable`. URL to use for health check monitoring. If the web proxy can't connect to this URL, it will assume that forwarding server is down. The default is set to `http://www.google.com`.

server-down-option {block | pass}

Action to take when the forwarding server is down:

- **block:** Blocks sessions until the server comes back up (set by default).
 - **pass:** Allows sessions to connect to their destination.
-

comment [string]

Optional comments.

web-proxy forward-server-group

Use this command to configure a load-balanced group of web proxy forward servers.

```
config web-proxy forward-server-group
  edit { name }
  # Configure a forward server group consisting or multiple forward servers. Supports failover and load balancing.
  set name { string }  Configure a forward server group consisting one or multiple forward servers. Supports failover and load balancing. size
[63]
  set affinity { enable | disable }  Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the for-
ward-server-affinity-timeout is reached (under web-proxy global).
  set ldb-method { weighted | least-session }  Load balance method: weighted or least-session.
  weighted      Load balance traffic to forward servers based on assigned weights.
  least-session Send new sessions to the server with lowest session count.
  set group-down-option { block | pass }  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.
  block Block sessions until at least one server in the group is back up.
  pass  Pass sessions to their destination bypassing servers in the forward server group.
config server-list
  edit { name }
  # Add web forward servers to a list to form a server group. Optionally assign weights to each server.
  set name { string }  Forward server name. size[63] - datasource(s): web-proxy.forward-server.name
  set weight { integer }  Optionally assign a weight of the forwarding server for weighted load balancing (1 - 100, default = 10)
range[1-100]
  next
next
end
```

config server-list

A configuration method to determine the load balancing weight for web proxy forwarding servers.

Note: You can only create entries if a web proxy forwarding server has already been created on the FortiGate. To do so, go to **Network > Explicit Proxy > Web Proxy Forwarding Servers** and select **Create New**.

weight <weight>

Weight (or ratio) of this server for load balancing. Set the value between 1-100. The default is set to 10.

affinity {enable | disable}

Enable (by default) or disable attaching source-ip's traffic to assigned forward-server until the `forward-server-affinity-timeout` is reached (see [web-proxy global](#)).

ldb-method {weighted | least-session}

Load-balancing method:

- **weighted**: Distribute to server based on weight (set by default).
- **least-session**: Distribute to server with lowest session count.

group-down-option {block | pass}

Action to take if all forward servers are down:

- **block**: Blocks traffic (set by default).
- **pass**: Passes traffic through.

web-proxy global

Use this command to configure global web proxy settings that control how the web proxy functions and handles web traffic. Typically, you should not have to change the default settings of this command. Also, if your FortiGate is operating with multiple VDOMS, these settings affect all VDOMS.

```
config web-proxy global
    set proxy-fqdn { string } Fully Qualified Domain Name (FQDN) that clients connect to (default = default.fqdn) to connect to the explicit web proxy. size[255]
    set max-request-length { integer } Maximum length of HTTP request line (2 - 64 Kbytes, default = 4). range[2-64]
    set max-message-length { integer } Maximum length of HTTP message, not including body (16 - 256 Kbytes, default = 32). range[16-256]
    set strict-web-check { enable | disable } Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP 1.1.
    set forward-proxy-auth { enable | disable } Enable/disable forwarding proxy authentication headers.
    set tunnel-non-http { enable | disable } Enable/disable allowing non-HTTP traffic. Allowed non-HTTP traffic is tunneled.
    set unknown-http-version { reject | tunnel | best-effort } Action to take when an unknown version of HTTP is encountered: reject, allow (tunnel), or proceed with best-effort.
        reject Rejects requests with unknown HTTP version.
        tunnel Tunnels requests with unknown HTTP version.
        best-effort Allow unknown HTTP requests and process them using best efforts.
    set forward-server-affinity-timeout { integer } Period of time before the source IP's traffic is no longer assigned to the forwarding server (6 - 60 min, default = 30). range[6-60]
    set max-waf-body-cache-length { integer } Maximum length of HTTP messages processed by Web Application Firewall (WAF) (10 - 1024 Kbytes, default = 100). range[10-1024]
    set webproxy-profile { string } 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. size[63] - datasource(s): web-proxy.profile.name
    set learn-client-ip { enable | disable } Enable/disable learning the client's IP address from headers.
    set learn-client-ip-from-header { true-client-ip | x-real-ip | x-forwarded-for } Learn client IP address from the specified headers.
        true-client-ip Learn the client IP address from the True-Client-IP header.
        x-real-ip Learn the client IP address from the X-Real-IP header.
        x-forwarded-for Learn the client IP address from the X-Forwarded-For header.
config learn-client-ip-srcaddr
    edit { name }
        # Source address name (srcaddr or srcaddr6 must be set).
        set name { string } Address name. size[64] - datasource(s): firewall.address.name,firewall.addrgrp.name
    next
config learn-client-ip-srcaddr6
    edit { name }
        # IPv6 Source address name (srcaddr or srcaddr6 must be set).
        set name { string } Address name. size[64] - datasource(s): firewall.address6.name,firewall.addrgrp6.name
```

```
    next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

proxy-fqdn <fqdn>

FQDN for the proxy for that clients use to connect. The default is set to `default.fqdn`.

max-request-length <kb>

Maximum length in kilobytes (kB) of the HTTP request line. Set the value between 2-64. The default is set to 4.

max-message-length <kb>

Maximum length in kB of the HTTP message, not including the body. Set the value between 16-256. The default is set to 32.

strict-web-check {enable | disable}

Enable or disable (by default) the blocking of web sites that send incorrect headers that don't conform to HTTP 1.1 (see [RFC 2616](#) for more information). Enabling this option may block some commonly used websites.

forward-proxy-auth {enable | disable}

Enable or disable (by default) the forwarding of proxy authentication headers. Note that this option is only practical when in explicit mode, because proxy authentication headers are always forwarded when in transparent mode. By default, in explicit mode, proxy authentication headers are blocked by the explicit web proxy. Therefore, enable this entry if you need to allow proxy authentication through the explicit web proxy.

tunnel-non-http {enable | disable}

Enable (by default) or disable the allowance of non-HTTP traffic.

unknown-http-version {reject | tunnel | best-effort}

Action to take when an unknown version of HTTP is encountered. Unknown HTTP sessions are those that don't comply with HTTP 0.9, 1.0, 1.1.

- **reject:** Rejects requests with unknown HTTP version.
- **tunnel:** Tunnels requests with unknown HTTP version.
- **best-effort:** Proceeds with best effort (set by default).

forward-server-affinity-timeout <minutes>

Period of time in minutes before the source IP's traffic will no longer be assigned to the forward server. Set the value between 6-60 (or six minutes to one hour). The default is set to 30.

max-waf-body-cache-length <kb>

Maximum length in kB of HTTP message processed by the Web Application Firewall (WAF). Set the value between 10-1024 (or 10kB to just over 1MB). The default is set to 100.

webproxy-profile <name>

Web proxy profile name.

learn-client-ip {enable | disable}

Enable or disable (by default) the learning of client IP addresses from headers.

web-proxy profile

Use this command to configure web proxy profiles that control how the web proxy functions and handles web traffic.

```

config web-proxy profile
  edit { name }
  # Configure web proxy profiles.
  set name { string } Profile name. size[63]
  set header-client-ip { pass | add | remove } Actions to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or
removes the HTTP header.
    pass Forward the same HTTP header.
    add Add the HTTP header.
    remove Remove the HTTP header.
  set header-via-request { pass | add | remove } Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or
removes the HTTP header.
    pass Forward the same HTTP header.
    add Add the HTTP header.
    remove Remove the HTTP header.
  set header-via-response { pass | add | remove } Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or
removes the HTTP header.
    pass Forward the same HTTP header.
    add Add the HTTP header.
    remove Remove the HTTP header.
  set header-x-forwarded-for { pass | add | remove } Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards
(pass), adds, or removes the HTTP header.
    pass Forward the same HTTP header.
    add Add the HTTP header.
    remove Remove the HTTP header.
  set header-front-end-https { pass | add | remove } Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards
(pass), adds, or removes the HTTP header.
    pass Forward the same HTTP header.
    add Add the HTTP header.
    remove Remove the HTTP header.
  set strip-encoding { enable | disable } Enable/disable stripping unsupported encoding from the request header.
config headers
  edit { id }
  # Configure HTTP forwarded requests headers.
  set id { integer } HTTP forwarded header id. range[0-4294967295]
  set name { string } HTTP forwarded header name. size[79]

```

```
        set action { add-to-request | add-to-response | remove-from-request | remove-from-response } Action when HTTP the header forwarded.
            add-to-request      Add the HTTP header to request.
            add-to-response     Add the HTTP header to response.
            remove-from-request Remove the HTTP header from request.
            remove-from-response Remove the HTTP header from response.
        set content { string } HTTP header's content. size[255]
    next
end
```

Supplemental Information

The following section is for those commands that require further explanation.

header-client-ip {pass | add | remove}

Action to take on client IP in forwarded requests header. Set the action to one of the following:

- **pass:** Forwards the same HTTP header.
- **add:** Adds the HTTP header.
- **remove:** Removes the HTTP header.

The default is set to `pass`.

header-via-request {pass | add | remove}

Action to take on via-request header in forwarded requests. The default is set to `pass`.

header-via-response {pass | add | remove}

Action to take on via-response header in forwarded requests. The default is set to `pass`.

header-x-forwarded-for {pass | add | remove}

Action to take on X-Forwarded-For (XFF) header in forwarded requests. The default is set to `pass`. XFF is a common non-standard request field, used to identify originating IP addresses of clients, and is also an email-header indicating that an email was forwarded from one or more accounts.

header-front-end-https {pass | add | remove}

Action to take on Front-End-Https header in forwarded requests. The default is set to `pass`. The Front-End-Https header is used for communication between front-end and back-end servers for SSL and formulating URLs using HTTPS instead of HTTP.

strip-encoding {enable | disable}

Enable or disable (by default) stripping of unsupported encoding in request header.

config headers

Use this configuration method to define HTTP forwarded requests headers for action.

name <name>

HTTP forwarded header name.

action <action>

Action to take when HTTP header is forwarded:

- **add-to-request:** Add HTTP header to request (set by default).
- **add-to-response:** Add HTTP header to response.
- **remove-from-request:** Remove HTTP header from request.
- **remove-from-response:** Remove HTTP header from response.

content <content>

Enter the HTTP header content.

web-proxy url-match

Use this command to define URLs for forward-matching or cache exemption.

```
config web-proxy url-match
  edit { name }
  # Exempt URLs from web proxy forwarding and caching.
  set name { string }   Configure a name for the URL to be exempted. size[63]
  set status { enable | disable }  Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding and caching.
  set url-pattern { string }  URL pattern to be exempted from web proxy forwarding and caching. size[511]
  set forward-server { string }  Forward server name. size[35] - datasource(s): web-proxy.forward-server.name,web-proxy.forward-server-group.-
name
  set cache-exemption { enable | disable }  Enable/disable exempting this URL pattern from caching.
  set comment { string }  Comment. size[255]
  next
end
```

status {enable | disable}

Enable (by default) or disable per URL pattern web proxy forwarding and cache exemptions.

url-pattern <string>

The URL pattern.

forward-server <name>

Name of the forward server.

cache-exemption {enable | disable}

Enable or disable (by default) a cache exemption list. When enabled, the specified URL pattern will be exempted from caching.

comment [string]

Optional comments.

web-proxy wisp

Use this command to configure web proxy Websense wireless Internet service provider (WISP) servers.

```
config web-proxy wisp
  edit { name }
  # Configure Wireless Internet service provider (WISP) servers.
  set name { string } Server name. size[35]
  set comment { string } Comment. size[255]
  set outgoing-ip { ipv4 address any } WISP outgoing IP address.
  set server-ip { ipv4 address any } WISP server IP address.
  set server-port { integer } WISP server port (1 - 65535, default = 15868). range[1-65535]
  set max-connections { integer } Maximum number of web proxy WISP connections (4 - 4096, default = 64). range[4-4096]
  set timeout { integer } Period of time before WISP requests time out (1 - 15 sec, default = 5). range[1-15]
  next
end
```

comment [string]

Optional comments.

outgoing-ip <ip-address>

WISP outgoing IP address.

server-ip <ip-address>

WISP server IP address.

server-port <port>

WISP server port. Set the value between 1-65535. The default is set to 15868.

max-connections <integer>

Maximum number of web proxy WISP connections. Set the value between 4-4096. The default is set to 64.

timeout <seconds>

Period of time in seconds before WISP requests timeout. Set the value between 1-15. The default is set to 5.

wireless-controller

Use `config wireless-controller` to configure virtual wireless access points that can be associated with multiple physical wireless access points, thereby extending the range of your wireless network.

This section includes syntax for the following commands:

- `wireless-controller ap-status`
- `wireless-controller ble-profile`
- `wireless-controller bonjour-profile`
- `wireless-controller global`
- `wireless-controller inter-controller`
- `wireless-controller qos-profile`
- `wireless-controller setting`
- `wireless-controller timers`
- `wireless-controller vap`
- `wireless-controller vap-group`
- `wireless-controller wids-profile`
- `wireless-controller wtp`
- `wireless-controller wtp-group`
- `wireless-controller wtp-profile`

wireless-controller ap-status

Use this command to designate detected access points as either accepted, rogue, or rogue APs that are suppressed. To see information about detected access points, use the `get wireless-controller scan` command.

```
config wireless-controller ap-status
  edit { id }
  # Configure access point status (rogue | accepted | suppressed).
  set id { integer }   AP ID. range[0-4294967295]
  set bssid { mac address }   The Access Point's (AP's) BSSID.
  set ssid { string }   The Access Point's (AP's) SSID. size[32]
  set status { rogue | accepted | suppressed }   The Access Point's (AP's) status: rogue, accepted, or suppressed.
    rogue      Rogue AP.
    accepted   Accepted AP.
    suppressed Suppressed AP.
  next
end
```

bssid <mac-address>

The access point's basic service set identifier (BSSID), expressed as the AP's wireless MAC address.

ssid <name>

The access point's SSID, expressed as the network name for the wireless interface.

status {rogue | accepted | suppressed}

Status of the AP:

- **rogue:** Defines an AP as undesirable, but still available.
- **accepted:** Defines an AP as accepted in the wireless network.
- **suppressed:** Actively prevents users from connecting to these rogue APs.

If you have rogue APs in your network, you can choose to monitor them. See [Monitoring rogue APs](#) from our Online Help portal for more details.

wireless-controller ble-profile

Introduction.

```
config wireless-controller ble-profile
  edit { name }
  # Configure Bluetooth Low Energy profile.
  set name { string } Bluetooth Low Energy profile name. size[35]
  set comment { string } Comment. size[63]
  set advertising { ibeacon | eddystone-uid | eddystone-url } Advertising type.
    ibeacon iBeacon advertising.
    eddystone-uid Eddystone UID advertising.
    eddystone-url Eddystone URL advertising.
  set ibeacon-uuid { string } Universally Unique Identifier (UUID; automatically assigned but can be manually reset). size[63]
  set major-id { integer } Major ID. range[0-65535]
  set minor-id { integer } Minor ID. range[0-65535]
  set eddystone-namespace { string } Eddystone namespace ID. size[10]
  set eddystone-instance { string } Eddystone instance ID. size[6]
  set eddystone-url { string } Eddystone URL. size[127]
  set txpower { option } Transmit power level (default = 0).
    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)
  set beacon-interval { integer } Beacon interval (default = 100 msec). range[40-3500]
  set ble-scanning { enable | disable } Enable/disable Bluetooth Low Energy (BLE) scanning.
next
end
```

wireless-controller global

Use this command to configure global settings for physical access points, also known as WLAN Termination Points (WTPs), configured using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

```
config wireless-controller global
  set name { string } Name of the wireless controller. size[35]
  set location { string } Description of the location of the wireless controller. size[35]
  set max-retransmit { integer } Maximum number of tunnel packet retransmissions (0 - 64, default = 3). range[0-64]
  set data-ethernet-II { enable | disable } Configure the wireless controller to use Ethernet II or 802.3 frames with 802.3 data tunnel mode
(default = disable).
  set link-aggregation { enable | disable } Enable/disable calculating the CAPWAP transmit hash to load balance sessions to link aggregation
nodes (default = disable).
  set mesh-eth-type { integer } Mesh Ethernet identifier included in backhaul packets (0 - 65535, default = 8755). range[0-65535]
  set fiapp-eth-type { integer } Ethernet type for Fortinet Inter-Access Point Protocol (IAPP), or IEEE 802.11F, packets (0 - 65535, default =
5252). range[0-65535]
  set discovery-mc-addr { multicast ipv4 address } Multicast IP address for AP discovery (default = 244.0.1.140).
  set max-clients { integer } Maximum number of clients that can connect simultaneously (default = 0, meaning no limitation). range[0-4294967295]
  set rogue-scan-mac-adjacency { integer } Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detec-
tion (0 - 31, default = 7). range[0-31]
  set ipsec-base-ip { ipv4 address } Base IP address for IPsec VPN tunnels between the access points and the wireless controller (default =
169.254.0.1).
  set wtp-share { enable | disable } Enable/disable sharing of WTPs between VDOMs.
  set ap-log-server { enable | disable } Enable/disable configuring APs or FortiAPs to send log messages to a syslog server (default = disable).
  set ap-log-server-ip { ipv4 address } The IP address that APs or FortiAPs send log messages to.
  set ap-log-server-port { integer } The TCP port that APs or FortiAPs send log messages to. range[0-65535]
end
```

Supplemental Information

The following section is for those commands that require further explanation.

name <name>

Name for the wireless network.

location <location>

Location of the wireless network.

max-retransmit

Maximum number of retransmissions for tunnel packet. Set the value between 0-64. The default is set to 3.

data-ethernet-ll {enable | disable}

Enable or disable (by default) the use of Ethernet frame type with 802.3 data tunnel mode.

link-aggregation {enable | disable}

Enable or disable (by default) CAPWAP transmit hash calculation for selecting link aggregation slaves.

mesh-eth-type

Mesh identifier included in packets, especially useful if debugging is required. Set the value between 0-65535. The default is set to 8755.

fiapp-eth-type

Ethernet type for Fortinet Inter-Access Point Protocol (IAPP), or IEEE 802.11F, packets. Set the value between 0-65535. The default is set to 5252.

discovery-mc-addr <multicast-address>

Multicast IP address for AP discovery. The default is set to 244.0.1.140.

max-clients <number>

Maximum number of clients that can connect simultaneously. The default is set to 0, meaning no limitation.

rogue-scan-mac-adjacency

Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection. MAC adjacency can be used to help with rogue detection, as AP WiFi interface MAC addresses are usually in the same range as its wired MAC address. LAN and WiFi network MAC addresses are matched when they are within a defined numerical distance of each other. Set the value between 0-31. The default is set to 7.

ipsec-base-ip <value>

Base IP address for WTP IPsec VPN tunnel. The default is 169.254.0.1.

ap-log-server {enable | disable}

Enable or disable (by default) the AP log server.

ap-log-server-ip <ip>

AP log server IP address.

ap-log-server-port <port>

AP log server port number.

wireless-controller setting

Use this command to configure VDOM-specific options for the wireless controller.

```
config wireless-controller setting
  set account-id { string } FortiCloud customer account ID. size[63]
  set country { option } Country or region in which the FortiGate is located. The country determines the 802.11 bands and channels that are available.
    NA NO_COUNTRY_SET
    AL ALBANIA
    DZ ALGERIA
    AO ANGOLA
    AR ARGENTINA
    AM ARMENIA
    AU AUSTRALIA
    AT AUSTRIA
    AZ AZERBAIJAN
    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
    CL CHILE
    CN CHINA
    CO COLOMBIA
    CR COSTA RICA
    HR CROATIA
    CY CYPRUS
    CZ CZECH REPUBLIC
    DK DENMARK
    DO DOMINICAN REPUBLIC
    EC ECUADOR
```

EG EGYPT
SV EL SALVADOR
EE ESTONIA
FI FINLAND
FR FRANCE
GE GEORGIA
DE GERMANY
GR GREECE
GL GREENLAND
GD GRENADA
GU GUAM
GT GUATEMALA
HT HAITI
HN HONDURAS
HK HONG KONG
HU HUNGARY
IS ICELAND
IN INDIA
ID INDONESIA
IR IRAN
IE IRELAND
IL ISRAEL
IT ITALY
JM JAMAICA
JO JORDAN
KZ KAZAKHSTAN
KE KENYA
KP NORTH KOREA
KR KOREA REPUBLIC
KW KUWAIT
LV LATVIA
LB LEBANON
LI LIECHTENSTEIN
LT LITHUANIA
LU LUXEMBOURG
MO MACAU SAR
MK MACEDONIA, FYRO
MY MALAYSIA
MT MALTA
MX MEXICO
MC MONACO
MA MOROCCO
MZ MOZAMBIQUE

```
NP  NEPAL
NL  NETHERLANDS
AN  NETHERLANDS ANTILLES
AW  ARUBA
NZ  NEW ZEALAND
NO  NORWAY
OM  OMAN
PK  PAKISTAN
PA  PANAMA
PG  PAPUA NEW GUINEA
PY  PARAGUAY
PE  PERU
PH  PHILIPPINES
PL  POLAND
PT  PORTUGAL
PR  PUERTO RICO
QA  QATAR
RO  ROMANIA
RU  RUSSIA
RW  RWANDA
SA  SAUDI ARABIA
RS  REPUBLIC OF SERBIA
ME  MONTENEGRO
SG  SINGAPORE
SK  SLOVAKIA
SI  SLOVENIA
ZA  SOUTH AFRICA
ES  SPAIN
LK  SRI LANKA
SE  SWEDEN
SD  SUDAN
CH  SWITZERLAND
SY  SYRIAN ARAB REPUBLIC
TW  TAIWAN
TZ  TANZANIA
TH  THAILAND
TT  TRINIDAD AND TOBAGO
TN  TUNISIA
TR  TURKEY
AE  UNITED ARAB EMIRATES
UA  UKRAINE
GB  UNITED KINGDOM
US  UNITED STATES2
```

```
PS  UNITED STATES (PUBLIC SAFETY)
UY  URUGUAY
UZ  UZBEKISTAN
VE  VENEZUELA
VN  VIET NAM
YE  YEMEN
ZW  ZIMBABWE
JP  JAPAN14
CA  CANADA2

set duplicate-ssid { enable | disable }  Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.
set fapc-compatibility { enable | disable }  Enable/disable FAP-C series compatibility.
end
```

account-id

FortiCloud customer account ID.

country <country>

Country of operation for your wireless network. This determines the radio channels that are available. Note that you must set the country before you configure access point (WTP) profiles. To display all available countries, enter `set country ?`. The default is set to `US` (United States).

duplicate ssid

Enable or disable (by default) allowance of VAPs to use the same SSID name in the same VDOM.

wireless-controller timers

Use this command to alter global timers for physical access points, also known as WTPs configured using CAPWAP.

```
config wireless-controller timers
  set echo-interval { integer }   Time between the WTP, AP, or FortiAP sends Echo Requests after joining the wireless controller (1 - 255 sec,
default = 30). range[1-255]
  set discovery-interval { integer }   Time between discovery requests (2 - 180 sec, default = 5). range[2-180]
  set client-idle-timeout { integer }   Time after which a client is considered idle and times out (20 - 3600 sec, default = 300, 0 for no
timeout). range[20-3600]
  set rogue-ap-log { integer }   Time between logging rogue AP messages if periodic rogue AP logging is configured (0 - 1440 min, default = 0).
range[0-1440]
  set fake-ap-log { integer }   Time between recording logs about fake APs if periodic fake AP logging is configured (0 - 1440 min, default = 1).
range[1-1440]
  set darrp-optimize { integer }   Time for running Dynamic Automatic Radio Resource Provisioning (DARRP) optimizations (0 - 86400 sec, default =
1800). range[0-86400]
  set darrp-day { option }   Weekday on which to run DARRP optimization.
    sunday   Sunday.
    monday   Monday.
    tuesday   Tuesday.
    wednesday Wednesday.
    thursday Thursday.
    friday   Friday.
    saturday Saturday.
config darrp-time
  edit { time }
    # Time at which DARRP optimizations run (you can add up to 8 times).
    set time { string }   Time. size[5]
  next
  set sta-stats-interval { integer }   Time between running client (station) reports (1 - 255 sec, default = 1). range[1-255]
  set vap-stats-interval { integer }   Time between running Virtual Access Point (VAP) reports (1 - 255 sec, default = 15). range[1-255]
  set radio-stats-interval { integer }   Time between running radio reports (1 - 255 sec, default = 15). range[1-255]
  set sta-capability-interval { integer }   Time between running station capability reports (1 - 255 sec, default = 30). range[1-255]
  set sta-locate-timer { integer }   Time between running client presence flushes to remove clients that are listed but no longer present (0 -
86400 sec, default = 1800). range[0-86400]
  set ipsec-intf-cleanup { integer }   Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected (30 - 3600 sec, default =
120). range[30-3600]
  set ble-scan-report-intv { integer }   Time between running Bluetooth Low Energy (BLE) reports (10 - 3600 sec, default = 30). range[10-3600]
```

end

echo-interval

Period of time in seconds before the WTP sends Echo Requests after joining AC. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 30.

discovery-interval

Period of time in seconds between discovery requests. Set the value between 2-180 (or two seconds to three minutes). The default is set to 5.

client-idle-timeout

Period of time in seconds before client is considered idle and timeouts. Set the value between 20-3600 (or 20 seconds to one hour), or 0 for no timeout. The default is set to 300.

rogue-ap-log

Intervals of time in minutes for periodic logging of rogue APs. Set the value between 0-1440 (or no logging to one day). The default is set to 0.

fake-ap-log

Intervals of time in minutes for periodic logging of fake APs. Fake APs serve to attract potential hackers and other intruders so as to collect information about them. Set the value between 0-1440 (or no interval to one day). The default is set to 1.

darrp-optimize

Intervals of time in seconds for Dynamic Automatic Radio Resource Provisioning (DARRP) optimization. Set the value between 0-86400 (or no interval to one day). The default is set to 1800.

sta-stats-interval

Intervals of time in seconds between station statistic reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 1.

vap-stats-interval

Intervals of time in seconds between VAP statistic reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 15.

radio-stats-interval

Intervals of time in seconds between radio statistic reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 15.

sta-capability-interval

Intervals of time in seconds between station capability reports. Set the value between 1-255 (or one second to four minutes and 25 seconds). The default is set to 30.

sta-locate-timer

Intervals of time in seconds between station presence flushes by the WTP. Set the value between 0-86400 (or no interval to one day). The default is set to 1800.

ipsec-intf-cleanup

Time period to keep IPsec VPN interface after WTP sessions are disconnected (default = 120 sec).

wireless-controller vap-group

Use this command to add multiple SSIDs to VAP groups.

```
config wireless-controller vap-group
  edit { name }
  # Configure virtual Access Point (VAP) groups.
  set name { string }   Group Name size[35]
  set comment { string } Comment. size[255]
  config vaps
    edit { name }
    # List of SSIDs to be included in the VAP group.
    set name { string }   vap name size[35] - datasource(s): wireless-controller.vap.name
    next
  next
end
```

append vaps <ssid>

Append SSIDs to be included in the VAP group.

comment [string]

Optional comments.

vaps <ssids>

List of SSIDs to be included in the VAP group.

wireless-controller wids-profile

Use this command to configured Wireless Intrusion Detection (WIDS) profiles.

```

config wireless-controller wids-profile
  edit { name }
  # Configure wireless intrusion detection system (WIDS) profiles.
  set name { string } WIDS profile name. size[35]
  set comment { string } Comment. size[63]
  set sensor-mode { disable | foreign | both } Disable this WIDS profile or enable it and select the WiFi channels to monitor for attacks
(default = disable).
    disable Disable the WIDS profile.
    foreign Enable the WIDS profile and monitor foreign channels for WiFi attacks. Foreign channels are not supported for the country or
region the AP is configured for.
    both Enable the WIDS profile and monitor both foreign and home channels channels for WiFi attacks. Select this option to monitor
all WiFi channels.
  set ap-scan { disable | enable } Enable/disable rogue AP detection.
  set ap-bgscan-period { integer } Period of time between background scans (60 - 3600 sec, default = 600). range[60-3600]
  set ap-bgscan-intv { integer } Period of time between scanning two channels (1 - 600 sec, default = 1). range[1-600]
  set ap-bgscan-duration { integer } Listening time on a scanning channel (10 - 1000 msec, default = 20). range[10-1000]
  set ap-bgscan-idle { integer } Period of idle-time before channel scanning (0 - 1000 msec, default = 0). range[0-1000]
  set ap-bgscan-report-intv { integer } Period of time in seconds between background scan reports (15 - 600, default = 30). range[15-600]
  set ap-bgscan-disable-day { option } Optionally turn off scanning for one or more days of the week. Separate the days with a space. By
default, no days are set.
    sunday Sunday.
    monday Monday.
    tuesday Tuesday.
    wednesday Wednesday.
    thursday Thursday.
    friday Friday.
    saturday Saturday.
  set ap-bgscan-disable-start { string } Start time, using a 24-hour clock in the format of hh:mm, for disabling background scanning (default
= 00:00).
  set ap-bgscan-disable-end { string } End time, using a 24-hour clock in the format of hh:mm, for disabling background scanning (default =
00:00).
  set ap-fgscan-report-intv { integer } Period of time in seconds between foreground scan reports (15 - 600, default = 15). range[15-600]
  set ap-scan-passive { enable | disable } Enable/disable passive scanning on all channels. Disable means do not send probe request on any
channels (default = disable).
  set ap-auto-suppress { enable | disable } Enable/disable on-wire rogue AP auto-suppression (default = disable).

```

```

set wireless-bridge { enable | disable } Enable/disable wireless bridge detection (default = disable).
set deauth-broadcast { enable | disable } Enable/disable broadcasting de-authentication detection (default = disable).
set null-ssid-probe-resp { enable | disable } Enable/disable null SSID probe response detection (default = disable).
set long-duration-attack { enable | disable } Enable/disable long duration attack detection based on user configured threshold (default =
disable).
set long-duration-thresh { integer } Threshold value for long duration attack detection (1000 - 32767 usec, default = 8200). range[1000-
32767]
set invalid-mac-oui { enable | disable } Enable/disable invalid MAC OUI detection.
set weak-wep-iv { enable | disable } Enable/disable weak WEP IV (Initialization Vector) detection (default = disable).
set auth-frame-flood { enable | disable } Enable/disable authentication frame flooding detection (default = disable).
set auth-flood-time { integer } Number of seconds after which a station is considered not connected. range[5-120]
set auth-flood-thresh { integer } The threshold value for authentication frame flooding. range[1-100]
set assoc-frame-flood { enable | disable } Enable/disable association frame flooding detection (default = disable).
set assoc-flood-time { integer } Number of seconds after which a station is considered not connected. range[5-120]
set assoc-flood-thresh { integer } The threshold value for association frame flooding. range[1-100]
set spoofed-death { enable | disable } Enable/disable spoofed de-authentication attack detection (default = disable).
set asleep-attack { enable | disable } Enable/disable asleep attack detection (default = disable).
set eapol-start-flood { enable | disable } Enable/disable EAPOL-Start flooding (to AP) detection (default = disable).
set eapol-start-thresh { integer } The threshold value for EAPOL-Start flooding in specified interval. range[2-100]
set eapol-start-intv { integer } The detection interval for EAPOL-Start flooding (1 - 3600 sec). range[1-3600]
set eapol-logoff-flood { enable | disable } Enable/disable EAPOL-Logoff flooding (to AP) detection (default = disable).
set eapol-logoff-thresh { integer } The threshold value for EAPOL-Logoff flooding in specified interval. range[2-100]
set eapol-logoff-intv { integer } The detection interval for EAPOL-Logoff flooding (1 - 3600 sec). range[1-3600]
set eapol-succ-flood { enable | disable } Enable/disable EAPOL-Success flooding (to AP) detection (default = disable).
set eapol-succ-thresh { integer } The threshold value for EAPOL-Success flooding in specified interval. range[2-100]
set eapol-succ-intv { integer } The detection interval for EAPOL-Success flooding (1 - 3600 sec). range[1-3600]
set eapol-fail-flood { enable | disable } Enable/disable EAPOL-Failure flooding (to AP) detection (default = disable).
set eapol-fail-thresh { integer } The threshold value for EAPOL-Failure flooding in specified interval. range[2-100]
set eapol-fail-intv { integer } The detection interval for EAPOL-Failure flooding (1 - 3600 sec). range[1-3600]
set eapol-pre-succ-flood { enable | disable } Enable/disable premature EAPOL-Success flooding (to STA) detection (default = disable).
set eapol-pre-succ-thresh { integer } The threshold value for premature EAPOL-Success flooding in specified interval. range[2-100]
set eapol-pre-succ-intv { integer } The detection interval for premature EAPOL-Success flooding (1 - 3600 sec). range[1-3600]
set eapol-pre-fail-flood { enable | disable } Enable/disable premature EAPOL-Failure flooding (to STA) detection (default = disable).
set eapol-pre-fail-thresh { integer } The threshold value for premature EAPOL-Failure flooding in specified interval. range[2-100]
set eapol-pre-fail-intv { integer } The detection interval for premature EAPOL-Failure flooding (1 - 3600 sec). range[1-3600]
set deauth-unknown-src-thresh { integer } Threshold value per second to deauth unknown src for DoS attack (0: no limit). range[0-65535]
next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

comment [string]

Optional comments.

sensor-mode {enable | disable}

Enable or disable (by default) radio sensor mode.

ap-scan {enable | disable}

Enable or disable (by default) rogue AP scanning. Once enabled, configure a series of AP scanning options (see entries below).

ap-bgscan-period <seconds>

Note: This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between background scans. Set the value between 60-3600 (or one minute to one hour). The default is set to 600 (or ten minutes).

ap-bgscan-intv <seconds>

Note: This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between two scanning channels. Set the range between 1-600 (or one seconds to ten minutes). The default is set to 1.

ap-bgscan-duration <milliseconds>

Note: This entry is only available when `ap-scan` is set to `enable`. Listening time in milliseconds on a scanning channel. Set the value between 10-1000. The default is set to 20.

ap-bgscan-idle <milliseconds>

Note: This entry is only available when `ap-scan` is set to `enable`. Period of idle-time in milliseconds before channel scanning. Set the value between 0-1000. The default is set to 0.

ap-bgscan-report-intv <seconds>

Note: This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between background scan reports. Set the value between 15-600 (or 15 seconds to ten minutes). The default is set to 30.

ap-bgscan-disable-day {sunday | monday | tuesday | wednesday | thursday | friday | saturday}

Note: This entry is only available when `ap-scan` is set to `enable`. Days of the week when background scanning is *disabled*. By default, no days are set. When this entry is set (to any number of days), use the `ap-bgscan-disable-start` and `ap-bgscan-disable-end` entries to determine start and end times; the period between these two times is when background scanning is disabled.

ap-bgscan-disable-start <hh:mm>

Note: This entry is only available when `ap-bgscan-disable-day` is configured. Start time, in the format of hh:mm, for disabling background scanning. The default is set to 00:00.

ap-bgscan-disable-end <hh:mm>

Note: This entry is only available when `ap-bgscan-disable-day` is configured. End time, in the format of hh:mm, for disabling background scanning. The default is set to 00:00.

ap-fgscan-report-intv <seconds>

Note: This entry is only available when `ap-scan` is set to `enable`. Period of time in seconds between foreground scan reports. Set the value between 15-600 (or 15 seconds to ten minutes). The default is set to 15.

ap-scan-passive {enable | disable}

Note: This entry is only available when `ap-scan` is set to `enable`. Enable or disable (by default) passive scanning on all channels.

rogue-scan {enable | disable}

Note: This entry is only available when `ap-scan` is set to `enable`. Enable or disable (by default) rogue AP on-wire scan.

wireless-bridge {enable | disable}

Enable or disable (by default)

death-broadcast {enable | disable}

Enable or disable (by default) detection of wireless bridge operation, used to raise awareness if your network *doesn't* use a wireless bridge.

null-ssid-probe-resp {enable | disable}

Enable or disable (by default) null SSID probe response detection.

long-duration-attack {enable | disable}

Enable or disable (by default) long-duration attack detection. When enabled, use the `long-duration-thresh` entry to define the threshold.

long-duration-thresh <milliseconds>

Duration of time in milliseconds for long-duration attack detection. Set the value between 1000-32767 (or one second to over 32 seconds). The default is set to 8200 (or just over eight seconds).

invalid-mac-oui {enable | disable}

Enable or disable (by default) detection of spoofed MAC addresses. The first three bytes should indicate a known manufacturer.

weak-wep-iv {enable | disable}

Enable or disable (by default) detection of APs using weak WEP encryption.

auth-frame-flood {enable | disable}

Enable or disable (by default) detection of authentication frame flood attacks.

assoc-frame-flood {enable | disable}

Enable or disable (by default) detection of association frame flood attacks.

spoofed-deauth {enable | disable}

Enable or disable (by default) detection of spoofed deauthentication packets.

asleap-attack {enable | disable}

Enable or disable (by default) detection of asleap attacks, attempts to crack Lightweight Extensible Authentication Protocol (LEAP) security. LEAP is a wireless LAN authentication method that allows clients to re-authenticate frequently, giving the client a new WEP key each time. Enable or disable (by default) detection of asleap attacks, attempts to crack Lightweight Extensible Authentication Protocol (LEAP) security. LEAP is a wireless LAN authentication method that allows clients to re-authenticate frequently, giving the client a new WEP key each time.

eapol-start-flood {enable | disable}

Enable or disable (by default) detection of Extensible Authentication Protocol (EAP) over LAN (EAPoL) START flood attacks.

eapol-logoff-flood {enable | disable}

Enable or disable (by default) detection of EAPoL LOGOFF flood attacks.

eapol-succ-flood {enable | disable}

Enable or disable (by default) detection of EAPoL SUCC flood attacks.

eapol-fail-flood {enable | disable}

Enable or disable (by default) detection of EAPoL FAIL flood attacks. When enabled, use the `eapol-fail-intv` entry to define the detection interval.

eapol-fail-thresh <threshold>

Note: This entry is only available when `eapol-fail-flood` is set to `enable`. The EAPoL FAIL detection threshold interval. Set the value between 2-100. The default is set to 10.

eapol-fail-intv <seconds>

Note: This entry is only available when `eapol-fail-flood` is set to `enable`. Interval of time in seconds between EAP FAIL detection. Set the value between 1-3600 (or one second to one hour). The default is set to 1.

eapol-pre-succ-flood {enable | disable}

Enable or disable (by default) detection of EAPoL premature SUCC flood attacks.

eapol-pre-fail-flood {enable | disable}

Enable or disable (by default) detection of EAPoL premature FAIL flood attacks.

death-unknown-src-thresh <seconds>

Threshold value per second to deauthenticate unknown sources for DoS attacks. The default is set to 10. Set to 0 for no limitation.

wireless-controller wtp

Use this command to configure various wireless transaction protocol (WTP) settings, including VAP override options and physical APs for management by the wireless controller, also known as an Access Controller (AC). **Note:** Radio 2 settings are only available for FortiAP models with dual radios.

```
config wireless-controller wtp
  edit { wtp-id }
    # Configure a FortiAP by assigning it a pre-configured Wireless Termination Point (WTP) and then override WTP profile settings as required for the
    FortiAP.
    set wtp-id { string }   WTP ID. size[35]
    set index { integer }   Index (0 - 4294967295). range[0-4294967295]
    set admin { discovered | disable | enable }   Configure how the FortiGate operating as a wireless controller discovers and manages this WTP,
    AP or FortiAP.
    set name { string }     WTP, AP or FortiAP configuration name. size[35]
    set location { string }  Field for describing the physical location of the WTP, AP or FortiAP. size[35]
    set wtp-profile { string }  WTP profile name to apply to this WTP, AP or FortiAP. size[35] - datasource(s): wireless-controller.wtp-pro-
    file.name
    set wtp-mode { normal | remote }  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.
        normal Normal WTP, AP, or FortiAP.
        remote Remote WTP, AP, or FortiAP.
    set bonjour-profile { string }  Bonjour profile name. size[35] - datasource(s): wireless-controller.bonjour-profile.name
    set override-led-state { enable | disable }  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.
    set led-state { enable | disable }  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.
    set override-wan-port-mode { enable | disable }  Enable/disable overriding the wan-port-mode in the WTP profile.
    set wan-port-mode { wan-lan | wan-only }  Enable/disable using the FortiAP WAN port as a LAN port.
        wan-lan Use the FortiAP WAN port as a LAN port.
        wan-only Do not use the WAN port as a LAN port.
    set override-ip-fragment { enable | disable }  Enable/disable overriding the WTP profile IP fragment prevention setting.
    set ip-fragment-preventing { tcp-mss-adjust | icmp-unreachable }  Method by which IP fragmentation is prevented for CAPWAP tunneled control
    and data packets (default = tcp-mss-adjust).
        tcp-mss-adjust TCP maximum segment size adjustment.
        icmp-unreachable Drop packet and send ICMP Destination Unreachable
    set tun-mtu-uplink { integer }  Uplink tunnel maximum transmission unit (MTU) in octets (eight-bit bytes). Set the value to either 0 (by
    default), 576, or 1500. range[576-1500]
    set tun-mtu-downlink { integer }  Downlink tunnel MTU in octets. Set the value to either 0 (by default), 576, or 1500. range[576-1500]
    set override-split-tunnel { enable | disable }  Enable/disable overriding the WTP profile split tunneling setting.
```

```
set split-tunneling-acl-path { tunnel | local } Split tunneling ACL path is local/tunnel.
    tunnel Split tunneling ACL list traffic will be tunnel.
    local Split tunneling ACL list traffic will be local NATed.
set split-tunneling-acl-local-ap-subnet { enable | disable } Enable to use split-tunnel-acl to create an access control list of destinations that WTPs, FortiAPs or APs access locally instead of through the WiFi controller (default = disable).
config split-tunneling-acl
    edit { id }
        # Split tunneling ACL filter list.
        set id { integer } ID. range[0-4294967295]
        set dest-ip { ipv4 classnet } Destination IP and mask for the split-tunneling subnet.
    next
set override-lan { enable | disable } Enable to override the WTP profile LAN port setting.
set port-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port-ssid { string } Bridge LAN port to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port1-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 1 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port1-ssid { string } Bridge LAN port 1 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port2-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 2 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port2-ssid { string } Bridge LAN port 2 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port3-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 3 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port3-ssid { string } Bridge LAN port 3 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port4-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 4 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port4-ssid { string } Bridge LAN port 4 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port5-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 5 mode.
```

```

        offline      Offline.
        nat-to-wan    NAT WTP LAN port to WTP WAN port.
        bridge-to-wan Bridge WTP LAN port to WTP WAN port.
        bridge-to-ssid Bridge WTP LAN port to SSID.
set port5-ssid { string } Bridge LAN port 5 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port6-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 6 mode.
        offline      Offline.
        nat-to-wan    NAT WTP LAN port to WTP WAN port.
        bridge-to-wan Bridge WTP LAN port to WTP WAN port.
        bridge-to-ssid Bridge WTP LAN port to SSID.
set port6-ssid { string } Bridge LAN port 6 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port7-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 7 mode.
        offline      Offline.
        nat-to-wan    NAT WTP LAN port to WTP WAN port.
        bridge-to-wan Bridge WTP LAN port to WTP WAN port.
        bridge-to-ssid Bridge WTP LAN port to SSID.
set port7-ssid { string } Bridge LAN port 7 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port8-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 8 mode.
        offline      Offline.
        nat-to-wan    NAT WTP LAN port to WTP WAN port.
        bridge-to-wan Bridge WTP LAN port to WTP WAN port.
        bridge-to-ssid Bridge WTP LAN port to SSID.
set port8-ssid { string } Bridge LAN port 8 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set override-allowaccess { enable | disable } Enable to override the WTP profile management access configuration.
set allowaccess { telnet | http | https | ssh } Control management access to the managed WTP, FortiAP, or AP. Separate entries with a
space.
        telnet      TELNET access.
        http        HTTP access.
        https       HTTPS access.
        ssh         SSH access.
set override-login-passwd-change { enable | disable } Enable to override the WTP profile login-password (administrator password) setting.
set login-passwd-change { yes | default | no } Change or reset the administrator password of a managed WTP, FortiAP or AP (yes, default, or
no, Default = no).
        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.
set login-passwd { password_string } Set the managed WTP, FortiAP, or AP's administrator password. size[31]
set radio-id { integer } radio-id range[0-2]
set override-band { enable | disable } Enable to override the WTP profile band setting.
set band { option } WiFi band that Radio 2 operates on.
        802.11a     802.11a.
        802.11b     802.11b.
        802.11g     802.11g/b.

```



```

    802.11n          802.11n/g/b radio at 2.4GHz band.
    802.11n-5G      802.11n/a at 5GHz.
    802.11n,g-only 802.11n/g at 2.4GHz.
    802.11g-only   802.11g.
    802.11n-only   802.11n at 2.4GHz.
    802.11n-5G-only 802.11n at 5GHz.
    802.11ac       802.11ac/n/a radio.
    802.11ac,n-only 802.11ac/n.
    802.11ac-only  802.11ac.
set override-analysis { enable | disable } Enable to override the WTP profile spectrum analysis configuration.
set spectrum-analysis { enable | disable } Enable/disable spectrum analysis to find interference that would negatively impact wireless
performance.
set override-txpower { enable | disable } Enable to override the WTP profile power level configuration.
set auto-power-level { enable | disable } Enable/disable automatic power-level adjustment to prevent co-channel interference (default =
enable).
set auto-power-high { integer } Automatic transmission power high limit in decibels (dB) of the measured power referenced to one mil-
liwatt (mW), or dBm (10 - 17 dBm, default = 17). range[0-4294967295]
set auto-power-low { integer } Automatic transmission power low limit (1 - 17 dBm, default = 10). range[0-4294967295]
set power-level { integer } Radio power level as a percentage (0 - 100, default = 100). range[0-100]
set override-vaps { enable | disable } Enable to override WTP profile Virtual Access Point (VAP) settings.
set vap-all { enable | disable } Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = disable).
config vaps
  edit { name }
    # Manually selected list of Virtual Access Points (VAPs) (max = 8).
    set name { string } Virtual Access Point (VAP) name. size[35] - datasource(s): wireless-controller.vap-group.name,wireless-con-
troller.vap.name
  next
set override-channel { enable | disable } Enable to override WTP profile channel settings.
config channel
  edit { chan }
    # Selected list of wireless radio channels (1 - 11).
    set chan { string } Channel number. size[3]
  next
set radio-id { integer } radio-id range[0-2]
set override-band { enable | disable } Enable to override the WTP profile band setting.
set band { option } WiFi band that Radio 2 operates on.
    802.11a          802.11a.
    802.11b          802.11b.
    802.11g          802.11g/b.
    802.11n          802.11n/g/b radio at 2.4GHz band.
    802.11n-5G      802.11n/a at 5GHz.
    802.11n,g-only 802.11n/g at 2.4GHz.
    802.11g-only   802.11g.

```

```

        802.11n-only      802.11n at 2.4GHz.
        802.11n-5G-only  802.11n at 5GHz.
        802.11ac         802.11ac/n/a radio.
        802.11ac,n-only  802.11ac/n.
        802.11ac-only    802.11ac.
    set override-analysis { enable | disable }  Enable to override the WTP profile spectrum analysis configuration.
    set spectrum-analysis { enable | disable }  Enable/disable spectrum analysis to find interference that would negatively impact wireless
performance.
    set override-txpower { enable | disable }  Enable to override the WTP profile power level configuration.
    set auto-power-level { enable | disable }  Enable/disable automatic power-level adjustment to prevent co-channel interference (default =
enable).
    set auto-power-high { integer }  Automatic transmission power high limit in decibels (dB) of the measured power referenced to one mil-
liwatt (mW), or dBm (10 - 17 dBm, default = 17). range[0-4294967295]
    set auto-power-low { integer }  Automatic transmission power low limit (1 - 17 dBm, default = 10). range[0-4294967295]
    set power-level { integer }  Radio power level as a percentage (0 - 100, default = 100). range[0-100]
    set override-vaps { enable | disable }  Enable to override WTP profile Virtual Access Point (VAP) settings.
    set vap-all { enable | disable }  Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = disable).
    config vaps
        edit { name }
            # Manually selected list of Virtual Access Points (VAPs) (max = 8).
            set name { string }  Virtual Access Point (VAP) name. size[35] - datasource(s): wireless-controller.vap-group.name,wireless-con-
troller.vap.name
        next
    set override-channel { enable | disable }  Enable to override WTP profile channel settings.
    config channel
        edit { chan }
            # Selected list of wireless radio channels (1 - 11).
            set chan { string }  Channel number. size[3]
        next
    set image-download { enable | disable }  Enable/disable WTP image download.
    set mesh-bridge-enable { default | enable | disable }  Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.
    set coordinate-enable { enable | disable }  Enable/disable WTP coordinates.
    set coordinate-x { string }  X axis coordinate. size[15]
    set coordinate-y { string }  Y axis coordinate. size[15]
    next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

config {radio-1 | radio-2}

A configuration method to set various override options for Radio 1 and/or Radio 2.

override-band {enable | disable}

Enable or disable (by default) the override of a specific AP-mode radio band. When enabled, use the `band` entry to configure the band.

band {802.11b | 802.11g | 802.11n | 802.11n,g-only | 802.11g-only | 802.11n-only}

Note: This entry is only available when `override-band` is set to `enable`.

Band of AP-mode radio. Note that this entry becomes available at the same time as `channel` does. In order to set the band, `channel` must be empty. To do this, enter `unset channel`. The channel may then be set after the band.

override-txpower {enable | disable}

Enable or disable (by default) the override of transmission power. When enabled, use the `auto-power-level` and `power-level` entries to to configure further power level options.

auto-power-level {enable | disable}

Note: This entry is only available when `override-txpower` is set to `enable`.

Enable or disable (by default) automatic transmission power adjustment. When enabled, use the `auto-power-high` and `auto-power-low` entries to configure the high and low limitations. When disabled, use the `power-level` entry to configure the power level percentage.

auto-power-high <dBm>

Note: This entry is only available when `override-txpower` is set to `enable` and `auto-power-level` is then set to `enable`.

Automatic transmission power high limit in decibels (dB) of the measured power referenced to one milliwatt (mW), or dBm. Set the value between 10-17. The default is set to 17.

auto-power-low <dBm>

Note: This entry is only available when `override-txpower` is set to `enable` and `auto-power-level` is then set to `enable`.

Automatic transmission power low limit in dBm. Set the value between 1-17. The default is set to 10.

power-level <percentage>

Note: This entry is only available when `override-txpower` is set to `enable` and `auto-power-level` is then set to `disable`.

Radio power level as a percentage; as such, set the value between 0-100. The default is set to 100.

The maximum power level (i.e. 100%) will set to the regulatory maximum for your region, as determined by the country entry under `config wireless-controller setting`.

override-vaps {enable | disable}

Enable or disable (by default) the override of VAPs. When enabled, use the `vap-all` and `vaps` entries to configure the VAPs carried on the physical AP.

vap-all {enable | disable}

Note: This entry is only available when `override-vaps` is set to `enable`.

Enable or disable (by default) the automatic inheritance of all VAPs. If disabled, you can select specific VAPs by using the `vaps` entry (see below).

vaps <vaps>

Note: This entry is only available when `override-vaps` is set to `enable` and `vap-all` is then set to `disable`.

Specific VAPs carried on this physical AP. Separate each value with a space to add multiple VAPs. Values can also be added using `append`.

override-channel {enable | disable}

Enable or disable (by default) the override of channels. When enabled, use the `channel` entry to enter the channels used by the AP.

channel {1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11}

Note: This entry is only available when either `override-band` or `override-channel` are set to `enable`.

Wireless radio channels to override. Separate each value with a space to add multiple channels. Values can also be added using `append`.

config split-tunneling-acl

Note: This configuration method is only available when `split-tunneling-acl-local-ap-subnet` is set to `enable`.

A configuration method to set various split tunneling access control list (ACL) filter lists.

dest-ip <ipv4>

IPv4 destination address to be added to the ACL filter.

config lan

Note: This configuration method is only available when `override-lan` is set to `enable`.

A configuration method to set WTP port mode.

port-mode {offline | nat-to-wan | bridge-to-wan | bridge-to-ssid}

LAN port mode:

- **offline:** No port bridging (by default)
 - **nat-to-wan:** Bridge NAT to the incoming WAN interface
 - **bridge-to-wan:** Bridge all LAN ports to the WAN interface
 - **bridge-to-ssid:** Bridge all LAN ports to the SSID
-

admin {discovered | disable | enable}

Enable (by default) or disable the AC to provide service to this WTP, or have the WTP discovered through either discovery or join request messages.

name <name>

Name for the AP.

location <location>

Location of the AP.

wtp-profile <profile>

Name of the WTP profile to apply to this AP, as created under `config wireless-controller wtp-profile`.

wtp-mode {normal | remote}

AP 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.

override-led-state {enable | disable}

Enable or disable (by default) the override of LED state. When enabled, use the `led-state` entry to enable or disable use of LEDs on WTP.

led-state {enable | disable}

Note: This entry is only available when `override-led-state` is set to `enable`. Enable (by default) or disable the use of LEDs on WTP.

override-ip-fragment {enable | disable}

Enable or disable (by default) the override of IP fragmentation. When enabled, use the `ip-fragment-preventing`, `tun-mtu-uplink`, and `tun-mtu-downlink` entries to configure IP fragmentation settings.

ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}

Note: This entry is only available when `override-ip-fragment` is set to `enable`. Method by which IP fragmentation is prevented for CAPWAP tunneled control and data packets:

- **tcp-mss-adjust:** TCP maximum segment adjustment (by default).
 - **icmp-unreachable:** Drop packet and send an Internet Control Message Protocol (ICMP) Destination Unreachable error message.
-

tun-mtu-uplink <bytes>

Note: This entry is only available when `override-ip-fragment` is set to `enable`. Uplink tunnel maximum transmission unit (MTU) in octets (eight-bit bytes). An MTU is the largest size packet or frame that can be sent in a packet. Set the value to either 0 (by default), 576, or 1500.

tun-mtu-downlink <bytes>

Note: This entry is only available when `override-ip-fragment` is set to `enable`. Downlink tunnel MTU in octets. Set the value to either 0 (by default), 576, or 1500.

override-split-tunnel {enable | disable}

Enable or disable (by default) to override split-tunneling. When enabled, use the `split-tunneling-acl-local-ap-subnet` entry to enable/disable the configuration of ACL filter lists.

split-tunneling-acl-local-ap-subnet {enable | disable}

Note: This entry is only available when `override-split-tunnel` is set to `enable`. Enable or disable (by default) specified destinations to be accessed locally instead of through the WiFi controller. When enabled, the `split-tunneling-acl` configuration method will become available.

override-lan {enable | disable}

Enable or disable (by default) to override the WTP LAN port. When enabled, the `lan` configuration method will become available.

override-allowaccess {enable | disable}

Enable or disable (by default) to override management-access per protocol. When enabled, use the `allowaccess` entry to set the protocols permitted management-access.

allowaccess {telnet | http | https | ssh}

Note: This entry is only available when `override-allowaccess` is set to `enable`. Protocols to allow management-access to managed APs: `telnet`, `http`, `https`, and `ssh`. Separate each value with a space to add multiple protocols. Values can also be added using `append`.

override-login-passwd-change {enable | disable}

Enable or disable (by default) to override the login-password of managed APs. When enabled, use the `login-passwd-change` entry to determine password-change settings.

login-passwd-change {yes | default | no}

Note: This entry is only available when `override-login-passwd-change` is set to `enable`. Login password options:

- **yes:** Change login password of the managed AP
 - **default:** Reset login password to factory default
 - **no:** Do not change login password (by default)
-

image-download {enable | disable}

Enable (by default) or disable image download of WTP to the AP. In addition, you can use the following command to import the WTP firmware file from a TFTP server:

```
execute wireless-controller upload-wtp-image tftp <filename> <TFTP server address>
```

mesh-bridge-enable {default | enable | disable}

Enable, disable, or use default (by default) mesh Ethernet bridge local settings on the WTP (when the WTP is configured as a mesh branch-leaf AP).

coordinate-enable {enable | disable}

Enable or disable (by default) AP coordinates. When enabled, use the `coordinate-x` and `coordinate-y` entries to set the AP's X and Y axes.

coordinate-x <string>

Note: This entry is only available when `coordinate-enable` is set to `enable`. X axis coordinate of the AP.

coordinate-y <string>

Note: This entry is only available when `coordinate-enable` is set to `enable`. Y axis coordinate of the AP.

wireless-controller wtp-group

Use this command to add FortiAP models to WTP groups. A FortiAP can belong to no more than one FortiAP group. FortiAP Groups facilitate the application of FortiAP profiles to large numbers of FortiAPs. Through the VLAN Pool feature, a FortiAP Group can be associated with a VLAN to which WiFi clients will be assigned.

Note: A configuration method to add member devices to WTP groups created for the model's platform type. In order to add member devices, you must have already used the `platform-type` entry to add a FortiAP model, as per the example CLI configuration below; a group called **wtp-group-1** is created for a FortiAP-221C device and one member device is added:

```
config wireless-controller wtp-group
  edit wtp-group-1
    set platform-type 221C
    config wtp-list
      edit FP221C3X14019926
    end
  end
```

```
config wireless-controller wtp-group
  edit { name }
    # Configure WTP group.
    set name { string } WTP group name. size[35]
    set platform-type { option } FortiAP models to define the WTP group platform type.
      AP-11N Default 11n AP.
      220B FAP220B/221B.
      210B FAP210B.
      222B FAP222B.
      112B FAP112B.
      320B FAP320B.
      11C FAP11C.
      14C FAP14C.
      223B FAP223B.
      28C FAP28C.
      320C FAP320C.
      221C FAP221C.
      25D FAP25D.
      222C FAP222C.
      224D FAP224D.
```

```
214B    FK214B.
21D     FAP21D.
24D     FAP24D.
112D    FAP112D.
223C    FAP223C.
321C    FAP321C.
C220C   FAPC220C.
C225C   FAPC225C.
C221E   FAPC221E.
C226E   FAPC226E.
C23JD   FAPC23JD.
C24JE   FAPC24JE.
C21D    FAPC21D.
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.
S221E   FAPS221E.
S223E   FAPS223E.
U421E   FAPU421EV.
U423E   FAPU423EV.
U221EV  FAPU221EV.
U223EV  FAPU223EV.
U321EV  FAPU321EV.
U323EV  FAPU323EV.
config wtps
  edit { wtp-id }
  # WTP list.
  set wtp-id { string } WTP ID. size[35] - datasource(s): wireless-controller.wtp.wtp-id
  next
next
```

end

wireless-controller wtp-profile

Use this command to configure WTP profiles (or FortiAP Profiles as shown in the GUI), which define radio settings for a particular platform/FortiAP model. FortiAP units contain two radio transceivers, making it possible to provide both 2.4GHz 802.11b/g/n and 5GHz 802.11a/n service from the same AP. The profile also selects which SSIDs the APs will carry.

For example, a FortiAP can be configured to carry all SSIDs on one radio, while the other only carries a specific SSID. The radios can also be used for monitoring, used for the Rogue AP detection feature. See [Monitoring rogue APs](#) from our Online Help portal for more details, and [config wireless-controller wids-profile](#) for various AP detection settings.

Note: Radio 2 settings are only available for FortiAP models with dual radios.

```
config wireless-controller wtp-profile
  edit { name }
    # Configure Wireless Termination Point (WTP) profile (also called a FortiAP profile or an access profile (AP)) that defines radio settings for a
    particular platform (FortiAP model).
    set name { string } WTP (or FortiAP or AP) profile name. size[35]
    set comment { string } Comment. size[255]
    set type { option } WTP FortiAP or AP platform type. There are built-in WTP profiles for all supported FortiAP models. You can select a
    built in platform and customize it or create a new profile.
      AP-11N Default 11n AP.
      220B FAP220B/221B.
      210B FAP210B.
      222B FAP222B.
      112B FAP112B.
      320B FAP320B.
      11C FAP11C.
      14C FAP14C.
      223B FAP223B.
      28C FAP28C.
      320C FAP320C.
      221C FAP221C.
      25D FAP25D.
      222C FAP222C.
      224D FAP224D.
      214B FK214B.
      21D FAP21D.
      24D FAP24D.
```

```

112D  FAP112D.
223C  FAP223C.
321C  FAP321C.
C220C FAPC220C.
C225C FAPC225C.
C221E FAPC221E.
C226E FAPC226E.
C23JD FAPC23JD.
C24JE FAPC24JE.
C21D  FAPC21D.
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.
S221E FAPS221E.
S223E FAPS223E.
U421E FAPU421EV.
U423E FAPU423EV.
U221EV FAPU221EV.
U223EV FAPU223EV.
U321EV FAPU321EV.
U323EV FAPU323EV.

```

```

set ble-profile { string } Bluetooth Low Energy profile name. size[35] - datasource(s): wireless-controller.ble-profile.name
set wan-port-mode { wan-lan | wan-only } Enable/disable using a WAN port as a LAN port.
    wan-lan Enable using a WAN port as a LAN port.
    wan-only Disable using a WAN port as a LAN port.
set port-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.

```

```
set port-ssid { string } Bridge LAN port to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port1-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 1 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port1-ssid { string } Bridge LAN port 1 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port2-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 2 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port2-ssid { string } Bridge LAN port 2 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port3-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 3 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port3-ssid { string } Bridge LAN port 3 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port4-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 4 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port4-ssid { string } Bridge LAN port 4 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port5-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 5 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port5-ssid { string } Bridge LAN port 5 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port6-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 6 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port6-ssid { string } Bridge LAN port 6 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set port7-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 7 mode.
    offline Offline.
    nat-to-wan NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port7-ssid { string } Bridge LAN port 7 to SSID. size[15] - datasource(s): wireless-controller.vap.name
```

```

set port8-mode { offline | nat-to-wan | bridge-to-wan | bridge-to-ssid } LAN port 8 mode.
    offline      Offline.
    nat-to-wan   NAT WTP LAN port to WTP WAN port.
    bridge-to-wan Bridge WTP LAN port to WTP WAN port.
    bridge-to-ssid Bridge WTP LAN port to SSID.
set port8-ssid { string } Bridge LAN port 8 to SSID. size[15] - datasource(s): wireless-controller.vap.name
set energy-efficient-ethernet { enable | disable } Enable/disable use of energy efficient Ethernet on WTP.
set led-state { enable | disable } Enable/disable use of LEDs on WTP (default = disable).
config led-schedules
    edit { 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.
        set name { string } LED schedule name. size[35] - datasource(s): firewall.schedule.group.name,firewall.schedule.recurring.name
    next
set dtls-policy { clear-text | dtls-enabled | ipsec-vpn } WTP data channel DTLS policy (default = clear-text).
    clear-text   Clear Text Data Channel.
    dtls-enabled DTLS Enabled Data Channel.
    ipsec-vpn    IPsec VPN Data Channel.
set dtls-in-kernel { enable | disable } Enable/disable data channel DTLS in kernel.
set max-clients { integer } Maximum number of stations (STAs) supported by the WTP (default = 0, meaning no client limitation). range[0-4294967295]
set handoff-rssi { integer } Minimum received signal strength indicator (RSSI) value for handoff (20 - 30, default = 25). range[20-30]
set handoff-sta-thresh { integer } Threshold value for AP handoff (5 - 35, default = 30). range[5-35]
set handoff-roaming { enable | disable } Enable/disable client load balancing during roaming to avoid roaming delay (default = disable).
config deny-mac-list
    edit { id }
        # List of MAC addresses that are denied access to this WTP, FortiAP, or AP.
        set id { integer } ID. range[0-4294967295]
        set mac { mac address } A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.
    next
set ap-country { option } Country in which this WTP, FortiAP or AP will operate (default = US).
    NA NO_COUNTRY_SET
    AL ALBANIA
    DZ ALGERIA
    AO ANGOLA
    AR ARGENTINA
    AM ARMENIA
    AU AUSTRALIA
    AT AUSTRIA
    AZ AZERBAIJAN
    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
CL CHILE
CN CHINA
CO COLOMBIA
CR COSTA RICA
HR CROATIA
CY CYPRUS
CZ CZECH REPUBLIC
DK DENMARK
DO DOMINICAN REPUBLIC
EC ECUADOR
EG EGYPT
SV EL SALVADOR
EE ESTONIA
FI FINLAND
FR FRANCE
GE GEORGIA
DE GERMANY
GR GREECE
GL GREENLAND
GD GRENADA
GU GUAM
GT GUATEMALA
HT HAITI
HN HONDURAS
HK HONG KONG
HU HUNGARY
IS ICELAND
IN INDIA
ID INDONESIA
IR IRAN
IE IRELAND
IL ISRAEL
IT ITALY
JM JAMAICA

JO JORDAN
KZ KAZAKHSTAN
KE KENYA
KP NORTH KOREA
KR KOREA REPUBLIC
KW KUWAIT
LV LATVIA
LB LEBANON
LI LIECHTENSTEIN
LT LITHUANIA
LU LUXEMBOURG
MO MACAU SAR
MK MACEDONIA, FYRO
MY MALAYSIA
MT MALTA
MX MEXICO
MC MONACO
MA MOROCCO
MZ MOZAMBIQUE
NP NEPAL
NL NETHERLANDS
AN NETHERLANDS ANTILLES
AW ARUBA
NZ NEW ZEALAND
NO NORWAY
OM OMAN
PK PAKISTAN
PA PANAMA
PG PAPUA NEW GUINEA
PY PARAGUAY
PE PERU
PH PHILIPPINES
PL POLAND
PT PORTUGAL
PR PUERTO RICO
QA QATAR
RO ROMANIA
RU RUSSIA
RW RWANDA
SA SAUDI ARABIA
RS REPUBLIC OF SERBIA
ME MONTENEGRO
SG SINGAPORE

```

SK SLOVAKIA
SI SLOVENIA
ZA SOUTH AFRICA
ES SPAIN
LK SRI LANKA
SE SWEDEN
SD SUDAN
CH SWITZERLAND
SY SYRIAN ARAB REPUBLIC
TW TAIWAN
TZ TANZANIA
TH THAILAND
TT TRINIDAD AND TOBAGO
TN TUNISIA
TR TURKEY
AE UNITED ARAB EMIRATES
UA UKRAINE
GB UNITED KINGDOM
US UNITED STATES2
PS UNITED STATES (PUBLIC SAFETY)
UY URUGUAY
UZ UZBEKISTAN
VE VENEZUELA
VN VIET NAM
YE YEMEN
ZW ZIMBABWE
JP JAPAN14
CA CANADA2

```

```

set ip-fragment-preventing { tcp-mss-adjust | icmp-unreachable } Select how to prevent IP fragmentation for CAPWAP tunneled control and data packets (default = tcp-mss-adjust).

```

```

    tcp-mss-adjust TCP maximum segment size adjustment.

```

```

    icmp-unreachable Drop packet and send ICMP Destination Unreachable

```

```

set tun-mtu-uplink { integer } Uplink CAPWAP tunnel MTU in octets (0, 576, or 1500. Default = 0). range[576-1500]

```

```

set tun-mtu-downlink { integer } Downlink CAPWAP tunnel MTU in octets (0, 576, or 1500. Default = 0). range[576-1500]

```

```

set split-tunneling-acl-path { tunnel | local } Split tunneling ACL path is local/tunnel.

```

```

    tunnel Split tunneling ACL list traffic will be tunnel.

```

```

    local Split tunneling ACL list traffic will be local NATed.

```

```

set split-tunneling-acl-local-ap-subnet { enable | disable } Enable to use split-tunnel-acl to create an access control list of destinations that WTPs, FortiAPs or APs access locally instead of through the WiFi controller (default = disable).

```

```

config split-tunneling-acl

```

```

  edit { id }

```

```

    # Split tunneling ACL filter list.

```

```

      set id { integer } ID. range[0-4294967295]

```

```

        set dest-ip { ipv4 classnet } Destination IP and mask for the split-tunneling subnet.
    next
    set allowaccess { telnet | http | https | ssh } Control management access to the managed WTP, FortiAP, or AP. Separate entries with a
space.
        telnet TELNET access.
        http HTTP access.
        https HTTPS access.
        ssh SSH access.
    set login-passwd-change { yes | default | no } Change or reset the administrator password of a managed WTP, FortiAP or AP (yes, default, or
no, Default = no).
        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.
    set login-passwd { password_string } Set the managed WTP, FortiAP, or AP's administrator password. size[31]
    set lldp { enable | disable } Enable/disable Link Layer Discovery Protocol (LLDP) for the WTP, FortiAP, or AP (default = disable).
    set poe-mode { auto | 8023af | 8023at | power-adapter } Set the WTP, FortiAP, or AP's PoE mode.
        auto Automatically detect the PoE mode.
        8023af Use 802.3af PoE mode.
        8023at Use 802.3at PoE mode.
        power-adapter Use the power adapter to control the PoE mode.
    set radio-id { integer } radio-id range[0-2]
    set mode { disabled | ap | monitor | sniffer } Mode of radio 1. Radio 1 can be disabled, configured as an access point, a rogue AP mon-
itor, or a sniffer.
        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 Rogue AP 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 looking for Rogue AP activity.
    set band { option } WiFi band that Radio 1 operates on.
        802.11a 802.11a.
        802.11b 802.11b.
        802.11g 802.11g/b.
        802.11n 802.11n/g/b at 2.4GHz.
        802.11n-5G 802.11n/a at 5GHz.
        802.11ac 802.11ac/n/a.
        802.11n,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.
    set protection-mode { rtscts | ctsonly | disable } Enable/disable 802.11g protection modes to support backwards compatibility with
older clients (rtscts, ctsonly, disable).

```

```

    rtscts    Enable 802.11g protection RTS/CTS mode.
    ctsonly   Enable 802.11g protection CTS only mode.
    disable   Disable 802.11g protection mode.
set powersave-optimize { option } Enable client power-saving features such as TIM, AC VO, and OBSS etc.
    tim           TIM bit for client in power save mode.
    ac-vo         Use AC VO priority to send out packets in the power save queue.
    no-obss-scan  Do not put OBSS scan IE into beacon and probe response frames.
    no-11b-rate   Do not send frame using 11b data rate.
    client-rate-follow Adapt transmitting PHY rate with receiving PHY rate from a client.
set transmit-optimize { option } Packet transmission optimization options including power saving, aggregation limiting, retry limiting,
etc. All are enabled by default.
    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.
set amsdu { enable | disable } Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients
(default = enable).
set coexistence { enable | disable } Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).
set short-guard-interval { enable | disable } Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long
GI) of 800 ns.
set channel-bonding { 80MHz | 40MHz | 20MHz } Channel bandwidth: 80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coex-
istence.
    80MHz      80 MHz channel width.
    40MHz      40 MHz channel width.
    20MHz      20 MHz channel width.
set auto-power-level { enable | disable } Enable/disable automatic power-level adjustment to prevent co-channel interference (default =
enable).
set auto-power-high { integer } Automatic transmission power high limit in decibels (dB) of the measured power referenced to one mil-
liwatt (mW), or dBm (10 - 17 dBm, default = 17). range[0-4294967295]
set auto-power-low { integer } Automatic transmission power low limit (1 - 17 dNm, default = 10). range[0-4294967295]
set power-level { integer } Radio power level as a percentage (0 - 100, default = 100). range[0-100]
set dtim { integer } DTIM interval. The frequency to transmit Delivery Traffic Indication Message (or Map) (DTIM) messages (1 - 255,
default = 1). Set higher to save client battery life. range[1-255]
set beacon-interval { integer } Beacon interval, the interval between beacon packets (40 - 3500ms, default 100). range[0-65535]
set rts-threshold { integer } Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS
(256 - 2346, default = 2346). range[256-2346]
set frag-threshold { integer } Maximum packet size that can be sent without fragmentation (800 - 2346, default = 2346). range[800-2346]
set ap-sniffer-bufsize { integer } Sniffer buffer size (1 - 32 MB, default = 16). range[1-32]
set ap-sniffer-chan { integer } Channel on which to operate the sniffer (default = 6). range[0-4294967295]
set ap-sniffer-addr { mac address } MAC address to monitor.
set ap-sniffer-mgmt-beacon { enable | disable } Enable/disable sniffer on WiFi management Beacon frame (default = enable).
set ap-sniffer-mgmt-probe { enable | disable } Enable/disable sniffer on WiFi management probe frame (default = enable).

```

```

set ap-sniffer-mgmt-other { enable | disable } Enable/disable sniffer on WiFi management other frame (default = enable).
set ap-sniffer-ctl { enable | disable } Enable/disable sniffer on WiFi control frame (default = enable).
set ap-sniffer-data { enable | disable } Enable/disable sniffer on WiFi data frame (default = enable).
set channel-utilization { enable | disable } Enable/disable measuring channel utilization.
set spectrum-analysis { enable | disable } Enable/disable spectrum analysis to find interference that would negatively impact wireless
performance.
set wids-profile { string } Wireless Intrusion Detection System (WIDS) profile name to assign to the radio. size[35] - datasource(s):
wireless-controller.wids-profile.name
set darrp { enable | disable } Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is
always using the most optimal channel (default = disable).
set max-clients { integer } Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.
range[0-4294967295]
set max-distance { integer } Maximum expected distance between the AP and clients (0 - 54000 m, default = 0). range[0-54000]
set frequency-handoff { enable | disable } Enable/disable frequency handoff of clients to other channels (default = disable).
set ap-handoff { enable | disable } Enable/disable AP handoff of clients to other APs (default = disable).
set vap-all { enable | disable } Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = disable).
config vaps
  edit { name }
    # Manually selected list of Virtual Access Points (VAPs) (max = 8).
    set name { string } Virtual Access Point (VAP) name. size[35] - datasource(s): wireless-controller.vap-group.name,wireless-con-
troller.vap.name
  next
config channel
  edit { chan }
    # Selected list of wireless radio channels (1 - 11).
    set chan { string } Channel number. size[3]
  next
set call-admission-control { enable | disable } 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.
set call-capacity { integer } Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10). range[0-
60]
set bandwidth-admission-control { enable | disable } 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.
set bandwidth-capacity { integer } Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000). range[1-600000]
set radio-id { integer } radio-id range[0-2]
set mode { disabled | ap | monitor | sniffer } Mode of radio 2. Radio 2 can be disabled, configured as an access point, a rogue AP mon-
itor, or a sniffer.
  disabled Radio 2 is disabled.
  ap Radio 2 operates as an access point that allows WiFi clients to connect to your network.
  monitor Radio 2 operates as a Rogue AP monitor. As a monitor, the radio scans for other WiFi access points and adds them to the
Rogue AP monitor list.
  sniffer Radio 2 operates as a sniffer looking for Rogue AP activity.
set band { option } WiFi band that Radio 2 operates on.

```

```

802.11a      802.11a.
802.11b      802.11b.
802.11g      802.11g/b.
802.11n      802.11n/g/b at 2.4GHz.
802.11n-5G   802.11n/a at 5GHz.
802.11ac     802.11ac/n/a.
802.11n,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.

set protection-mode { rtscts | ctsonly | disable }  Enable/disable 802.11g protection modes to support backwards compatibility with
older clients (rtscts, ctsonly, disable).
    rtscts  Enable 802.11g protection RTS/CTS mode.
    ctsonly Enable 802.11g protection CTS only mode.
    disable Disable 802.11g protection mode.

set powersave-optimize { option }  Enable client power-saving features such as TIM, AC VO, and OBSS etc.
    tim          TIM bit for client in power save mode.
    ac-vo        Use AC VO priority to send out packets in the power save queue.
    no-obss-scan Do not put OBSS scan IE into beacon and probe response frames.
    no-11b-rate  Do not send frame using 11b data rate.
    client-rate-follow Adapt transmitting PHY rate with receiving PHY rate from a client.

set transmit-optimize { option }  Packet transmission optimization options including power saving, aggregation limiting, retry limiting,
etc. All are enabled by default.
    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.

set amsdu { enable | disable }  Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients
(default = enable).

set coexistence { enable | disable }  Enable/disable allowing both HT20 and HT40 on the same radio (default = enable).

set short-guard-interval { enable | disable }  Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long
GI) of 800 ns.

set channel-bonding { 80MHz | 40MHz | 20MHz }  Channel bandwidth: 80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coex-
istence.
    80MHz  80 MHz channel width.
    40MHz  40 MHz channel width.
    20MHz  20 MHz channel width.

set auto-power-level { enable | disable }  Enable/disable automatic power-level adjustment to prevent co-channel interference (default =
enable).

set auto-power-high { integer }  Automatic transmission power high limit in decibels (dB) of the measured power referenced to one

```

```

milliwatt (mW), or dBm (10 - 17 dBm, default = 17). range[0-4294967295]
    set auto-power-low { integer } Automatic transmission power low limit (1 - 17 dBm, default = 10). range[0-4294967295]
    set power-level { integer } Radio power level as a percentage (0 - 100, default = 100). range[0-100]
    set dtim { integer } DTIM interval. The frequency to transmit Delivery Traffic Indication Message (or Map) (DTIM) messages (1 - 255,
default = 1). Set higher to save client battery life. range[1-255]
    set beacon-interval { integer } Beacon interval, the interval between beacon packets (40 - 3500ms, default 100). range[0-65535]
    set rts-threshold { integer } Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS
(256 - 2346, default = 2346). range[256-2346]
    set frag-threshold { integer } Maximum packet size that can be sent without fragmentation (800 - 2346, default = 2346). range[800-2346]
    set ap-sniffer-bufsize { integer } Sniffer buffer size (1 - 32 MB, default = 16). range[1-32]
    set ap-sniffer-chan { integer } Channel on which to operate the sniffer (default = 6). range[0-4294967295]
    set ap-sniffer-addr { mac address } MAC address to monitor.
    set ap-sniffer-mgmt-beacon { enable | disable } Enable/disable sniffer on WiFi management Beacon frame (default = enable).
    set ap-sniffer-mgmt-probe { enable | disable } Enable/disable sniffer on WiFi management probe frame (default = enable).
    set ap-sniffer-mgmt-other { enable | disable } Enable/disable sniffer on WiFi management other frame (default = enable).
    set ap-sniffer-ctl { enable | disable } Enable/disable sniffer on WiFi control frame (default = enable).
    set ap-sniffer-data { enable | disable } Enable/disable sniffer on WiFi data frame (default = enable).
    set channel-utilization { enable | disable } Enable/disable measuring channel utilization.
    set spectrum-analysis { enable | disable } Enable/disable spectrum analysis to find interference that would negatively impact wireless
performance.
    set wids-profile { string } Wireless Intrusion Detection System (WIDS) profile name to assign to the radio. size[35] - datasource(s):
wireless-controller.wids-profile.name
    set darrp { enable | disable } Enable/disable Distributed Automatic Radio Resource Provisioning (DARRP) to make sure the radio is
always using the most optimal channel (default = disable).
    set max-clients { integer } Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.
range[0-4294967295]
    set max-distance { integer } Maximum expected distance between the AP and clients (0 - 54000 m, default = 0). range[0-54000]
    set frequency-handoff { enable | disable } Enable/disable frequency handoff of clients to other channels (default = disable).
    set ap-handoff { enable | disable } Enable/disable AP handoff of clients to other APs (default = disable).
    set vap-all { enable | disable } Enable/disable the automatic inheritance of all Virtual Access Points (VAPs) (default = disable).
config vaps
    edit { name }
        # Manually selected list of Virtual Access Points (VAPs) (max = 8).
        set name { string } Virtual Access Point (VAP) name. size[35] - datasource(s): wireless-controller.vap-group.name,wireless-con
troller.vap.name
    next
config channel
    edit { chan }
        # Selected list of wireless radio channels (1 - 11).
        set chan { string } Channel number. size[3]
    next
    set call-admission-control { enable | disable } 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.

```



```

    set call-capacity { integer }    Maximum number of Voice over WLAN (VoWLAN) phones supported by the radio (0 - 60, default = 10). range[0-60]

    set bandwidth-admission-control { enable | disable }    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.
    set bandwidth-capacity { integer }    Maximum bandwidth capacity allowed (1 - 600000 Kbps, default = 2000). range[1-600000]
    set ekahau-blink-mode { enable | disable }    Enable/disable Ekahua blink mode (also called AiRISTA Flow Blink Mode) to find the location of devices connected to a wireless LAN (default = disable).
    set ekahau-tag { mac address }    WiFi frame MAC address or WiFi Tag.
    set erc-server-ip { ipv4 address any }    IP address of Ekahua RTLS Controller (ERC).
    set erc-server-port { integer }    Ekahua RTLS Controller (ERC) UDP listening port. range[1024-65535]
    set aeroscout { enable | disable }    Enable/disable AeroScout Real Time Location Service (RTLS) support.
    set aeroscout-server-ip { ipv4 address any }    IP address of AeroScout server.
    set aeroscout-server-port { integer }    AeroScout server UDP listening port. range[1024-65535]
    set aeroscout-mu-factor { integer }    AeroScout Mobile Unit (MU) mode dilution factor (default = 20). range[0-4294967295]
    set aeroscout-mu-timeout { integer }    AeroScout MU mode timeout (0 - 65535 sec, default = 5). range[0-65535]
    set fortipresence { foreign | both | disable }    Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network (default = disable).
        foreign    FortiPresence monitors foreign channels only. Foreign channels are not supported for the country or region the AP is configured for.
        both        Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.
        disable    Disable FortiPresence.
    set fortipresence-server { ipv4 address any }    FortiPresence server IP address.
    set fortipresence-port { integer }    FortiPresence server UDP listening port (default = 3000). range[300-65535]
    set fortipresence-secret { password_string }    FortiPresence secret password (max. 16 characters). size[123]
    set fortipresence-project { string }    FortiPresence project name (max. 16 characters, default = fortipresence). size[16]
    set fortipresence-frequency { integer }    FortiPresence report transmit frequency (5 - 65535 sec, default = 30). range[5-65535]
    set fortipresence-rogue { enable | disable }    Enable/disable FortiPresence finding and reporting rogue APs.
    set fortipresence-unassoc { enable | disable }    Enable/disable FortiPresence finding and reporting unassociated stations.
    set station-locate { enable | disable }    Enable/disable client station locating services for all clients, whether associated or not (default = disable).
  next
end

```

Supplemental Information

The following section is for those commands that require further explanation.

config platform

A configuration method to assign the AP hardware type.

type <platform>

WTP platform type/model. For a full list of options, enter `set type ?` (or see `wireless-controller wtp-group`). The default is set to 220B.

config deny-mac-list

A configuration methods to deny specific wireless MAC addresses.

mac <mac-address>

Wireless MAC address to deny.

config split-tunneling-acl

A configuration method to set various split tunneling access control list (ACL) filter lists.

dest-ip <ipv4-netmask>

IPv4 destination address to be added to the ACL filter.

config {radio-1 | radio-2}

A configuration method to set various options for Radio 1 and/or Radio 2.

mode {disabled | ap | monitor | sniffer}

Radio mode for the AP:

- **disabled:** Radio is not used; *all* other entries are unavailable *except* `powersave-optimize`.
- **ap:** Radio provides wireless AP service (set by default); all other entries are available.
- **monitor:** Radio performs monitoring only; the only other entries available when this is set are `powersave-optimize`, `spectrum-analysis`, and `wids-profile`.
- **sniffer:** Radio performs scanning only; the only other entries available when this is set are `powersave-optimize`, all `ap-sniffer` related entries, and `spectrum-analysis`.

band {802.11b | 802.11g | 802.11n | 802.11n,g-only | 802.11g-only | 802.11n-only}

Band of AP-mode radio. The `n` bands operate at 2.4GHz.

protection-mode {rtscts | ctsonly | disable}

Note: This entry is only available under `radio-2`. 802.11g protection mode:

- **rtscts:** Enables 802.11g protection in Request to Send/Clear to Send (RTS/CTS) mode, reducing frame collisions
- **ctsonly:** Enables 802.11g protection in CTS mode
- **disable:** Disables 802.11g protection

powersave-optimize {tim | ac-vo | no-obss-scan | no-11b-rate | client-rate-follow}

Power-saving optimization options:

- **tim:** Set traffic indication map (TIM) bit for client in power save mode. TIM bit mask indicates to any sleeping listening stations if the AP has any buffered frames present.
- **ac-vo:** Use Access Category (AC) Voice (VO) priority to send packets in the power save queue. AC VO is one of the highest classes/priority levels used to ensure quality of service (QoS).
- **no-obss-scan:** Do not put Overlapping Basic Service Set (OBSS), or high-noise (i.e. non-802.11), scan IE into a Beacon or Probe Response frame.
- **no-11b-rate:** Do not send frame using 11b data rate.
- **client-rate-follow:** Adapt transmitted PHY rate to PHY rate received from client.

Separate each value with a space to add multiple values. Values can also be added using `append`.

ap-sniffer-bufsize <mb>

Note: This entry is only available when `mode` is set to `sniffer`. AP's sniffer buffer size in MB. Set the value between 1-32. The default is set to 16.

ap-sniffer-chan <channel>

Note: This entry is only available when `mode` is set to `sniffer`. Channel on which to operate the sniffer. The default is set to 6.

ap-sniffer-addr <mac-address>

Note: This entry is only available when `mode` is set to `sniffer`. MAC address to monitor.

ap-sniffer-mgmt-beacon {enable | disable}

Note: This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi management Beacon frame.

ap-sniffer-mgmt-probe {enable | disable}

Note: This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi management Probe frame.

ap-sniffer-mgmt-other {enable | disable}

Note: This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi management Other frame.

ap-sniffer-ctl {enable | disable}

Note: This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi Control frame.

ap-sniffer-data {enable | disable}

Note: This entry is only available when `mode` is set to `sniffer`. Enable (by default) or disable sniffer on WiFi Data frame.

transmit-optimize {disable | power-save | aggr-limit | retry-limit | send-bar}

Packet transmission optimization options (enabled by default; all options except `disable`):

- **disable:** No packet transmission optimization
- **power-save:** Tags client as operating in power save mode if excessive transmit retries occur
- **aggr-limit:** Sets a lower aggregation limit when the data rate is low
- **retry-limit:** Sets a lower retry limit when data rate is low
- **send-bar:** Limit transmission of Block Acknowledgement Request (BAR) frames

Separate each value with a space to add multiple values. Values can also be added using `append`.

amsdu {enable | disable}

Note: This entry is only available under `radio-2`. Enable (by default) or disable Aggregate MAC Service Data Unit (A-MSDU) support, allowing multiple frames to be combined into one larger frame.

coexistence {enable | disable}

Note: This entry is only available under `radio-2`. Enable (by default) or disable HT20/HT40 coexistence support, where bandwidths that use 20MHz and 40MHz can be used in the same channel.

channel-bonding {40MHz | 20MHz}

Note: This entry is only available under `radio-2`. Channel bandwidth: either 40MHz or 20MHz. Channels may use both by enabling the `coexistence` entry (see above).

auto-power-level {enable | disable}

Enable or disable (by default) automatic power-level adjustment to prevent co-channel interference. When enabled, use the `auto-power-high` and `auto-power-low` entries to configure the high and low limitations. When disabled, use the `power-level` entry to configure the power level percentage.

auto-power-high <dBm>

Note: This entry is only available when `auto-power-level` is set to `enable`. Automatic transmission power high limit in decibels (dB) of the measured power referenced to one milliwatt (mW), or dBm. Set the value between 10-17. The default is set to 17.

auto-power-low <dBm>

Note: This entry is only available when `auto-power-level` is set to `enable`. Automatic transmission power low limit in dBm. Set the value between 1-17. The default is set to 10.

power-level <percentage>

Note: This entry is only available when `auto-power-level` is set to `disable`. Radio power level as a percentage; as such, set the value between 0-100. The default is set to 100. The maximum power level (i.e. 100%) will set to the regulatory maximum for your region, as determined by the `country` entry under `config wireless-controller setting`.

dtim <interval>

Interval between an Delivery Traffic Indication Message (DTIM), a kind of TIM that informs clients about the presence of buffered multicast/broadcast data on the AP. Set the value between 1-255. The default is set to 1.

beacon-interval <milliseconds>

Interval between beacon packets. AP broadcast beacons or TIMs to synchronize wireless networks. Set the value between 40-3500 (or 40 milliseconds to 3.5 seconds). The default is set to 100 (or a tenth of a second). In an environment with high interference, a low `beacon-interval` value might improve network performance. In a location with few wireless nodes, you can increase this value.

rts-threshold <bytes>

Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS. This will consume more bandwidth, therefore reducing the throughput, however the more RTS packets there are the fewer instances of packet loss will occur. Set the value between 256-2346 (or 256 bytes to over 2kB). The default is set to 2346, meaning that effectively it will never be used, as the maximum packet size in Ethernet networks can only be 1518 bytes (including all headers and maximum data size).

channel-utilization {enable | disable}

Enable or disable (by default) channel utilization measurement.

frag-threshold <bytes>

Note: This entry is only available when `band` has been set. Maximum packet size that can be sent without fragmentation. Range is 800 to 2346 bytes. Set the value between 256-2346 (or 256 bytes to over 2kB).

spectrum-analysis {enable | disable}

Enable or disable (by default) spectrum analysis, a method for finding interference that would negatively impact wireless performance.

wids-profile

Note: This entry is only available when `mode` is set to either `ap` or `monitor`. WIDS profile name to assign to the radio, as configured under the `wireless-controller wids-profile` command.

darrp {enable | disable}

Enable or disable (by default) Distributed Automatic Radio Resource Provisioning (DARRP), a feature that autonomously and periodically determines the best-suited channel for wireless communication. This allows FortiAP units to select their channel so they do not interfere with each other in large-scale deployments. You can optimize DARRP further under the `wireless-controller timers` command.

max-clients <integer>

Maximum expected number of STAs supported by the radio. The default is set to 0.

max-distance <meters>

Maximum expected distance in meters between the AP and clients. This adjusts the ACK timeout to maintain throughput at the maximum distance. Set the value between 0-54000 (or no distance to just over 33.5 miles). The default is set to 0.

frequency-handoff {enable | disable}

Enable or disable (by default) frequency handoff of clients to other channels. When enabled, you can optimize handoff further by using the `handoff-rssi` and `handoff-sta-thresh` entries.

ap-handoff {enable | disable}

Enable or disable (by default) handoff of clients to other APs.

vap-all {enable | disable}

Enable (by default) or disable the automatic inheritance of all VAPs.

vaps <vaps>

Specific VAPs carried on this physical AP. Separate each value with a space to add multiple VAPs. A maximum of eight VAPs may be added. Values can also be added using `append`.

channel {1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11}

Wireless radio channels. Separate each value with a space to add multiple channels. Values can also be added using `append`.

config lbs

A configuration method to set various location based service (LBS) options.

ekahau-blink-mode {enable | disable}

Enable or disable (by default)

ekahau-tag <mac-address>

WiFi frame MAC address.

erc-energy-ip <ip-address>

IP address of the Ekahau real-time location system (RTLS) controller.

er-server-port <port>

Ekahau RTLS controller UDP listening port.

aeroscout {enable | disable}

Enable or disable (by default) AeroScout support.

aeroscout-server-ip <ip-address>

AeroScout server IP address.

aeroscout-server-port <port>

AeroScout server UDP listening port.

aeroscout-mu-factor <mu-factor>

AeroScout Mobile Unit (MU) mode dilution factor. The default is set to 20.

aeroscout-mu-timeout <seconds>

AeroScout MU mode timeout in seconds. Set the value between 0-65535 (or not timeout to over 18 hours). The default is set to 5.

fortipresence {enable | disable}

Enable or disable (by default) FortiPresence support.

fortipresence-server <ip-address>

FortiPresence server IP address.

fortipresence-port <port>

FortiPresence server UDP listening port. Set the value between 300-65535. The default is set to 3000.

fortipresence-secret <password>

FortiPresence secret password, with a maximum length of eight characters.

fortipresence-project <name>

Name of the FortiPresence project, with a maximum length of 16 characters. The default is set to `fortipresence`.

fortipresence-frequency <seconds>

FortiPresence report transmit frequency in seconds. Set the value between 5-65535 (or five seconds to over 18 hours). The default is set to 30.

fortipresence-rogue {enable | disable}

Enable or disable (by default) FortiPresence reporting Rogue APs.

fortipresence-unassoc {enable | disable}

Enable or disable (by default) FortiPresence reporting unassociated stations.

station-locate {enable | disable}

Enable or disable (by default) client station locating services for all clients, whether associated or not.

comment [string]

Optional comments.

led-state {enable | disable}

Enable (by default) or disable use of LEDs on WTP.

dtls-policy {clear-text | dtls-enabled}

WTP data channel DTLS policy.

- clear-text: (set by default).
- dtls-enabled:

Separate each value with a space to add multiple options. Values can also be added using `append`.

max-clients <number>

The default is set to 0, meaning there is no client limitation.

handoff-rssi <rssi>

Minimum received signal strength indicator (RSSI) value for handoff. Set the value between 20-30. The default is set to 25.

handoff-sta-thresh <threshold>

Threshold value for AP handoff. Set the value between 5-35. The default is set to 30.

handoff-roaming {enable | disable}

Enable (by default) or disable client load balancing during roaming to avoid roaming delay.

ap-country <country>

Country in which this AP will operate. To display all available countries, enter `set country ?`. The default is set to US (United States).

ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}

Method by which IP fragmentation is prevented for CAPWAP tunneled control and data packets:

- **tcp-mss-adjust:** TCP maximum segment adjustment (by default).
- **icmp-unreachable:** Drop packet and send an Internet Control Message Protocol (ICMP) Destination Unreachable error message.

Separate with a space to add both values. Values can also be added using `append`.

tun-mtu-uplink <bytes>

Uplink tunnel maximum transmission unit (MTU) in octets (eight-bit bytes). An MTU is the largest size packet or frame that can be sent in a packet. Set the value to either 0 (by default), 576, or 1500.

tun-mtu-downlink <bytes>

Downlink tunnel MTU in octets. Set the value to either 0 (by default), 576, or 1500.

split-tunneling-acl-local-ap-subnet {enable | disable}

Enable or disable (by default) specified destinations to be accessed locally instead of through the WiFi controller.

allowaccess {telnet | http | https | ssh}

Protocols to allow management-access to managed APs: `telnet`, `http`, `https`, and `ssh`. Separate each value with a space to add multiple protocols. Values can also be added using `append`.

login-passwd-change {yes | default | no}

Login password options:

- **yes:** Change login password of the managed AP
 - **default:** Reset login password to factory default
 - **no:** Do not change login password (by default)
-

When set to `yes`, use the `login-passwd` entry to determine the password of the managed AP.

login-passwd <password>

Note: This entry is only available when `login-passwd-change` is set to `yes`. Login password of the managed AP.

lldp {enable | disable}

Enable or disable (by default) Link Layer Discovery Protocol (LLDP), a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbours.

execute

The execute commands perform immediate operations on the FortiGate unit, including:

- Maintenance operations, such as back up and restore the system configuration, reset the configuration to factory settings, update antivirus and attack definitions, view and delete log messages, set the date and time.
- Network operations, such as view and clear DHCP leases, clear arp table entries, use `ping` or `traceroute` to diagnose network problems.
- Generate certificate requests and install certificates for VPN authentication.

backup

Back up the FortiGate configuration files, logs, or IPS user-defined signatures file to a TFTP or FTP server, USB disk, or a management station. Management stations can either be a FortiManager unit, or FortiGuard Analysis and Management Service. For more information, see ["fortiguard" on page 1](#) or ["central-management" on page 1](#).

When virtual domain configuration is enabled (in [global](#), `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin can restore the configuration from this file.

When you back up the system configuration from a regular administrator account, the backup file contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute backup config flash <comment>
execute backup config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config management-station <comment_str>
execute backup config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup config usb <filename_str> [<backup_password_str>]
execute backup config-with-forticlient-info usb-mode [<backup_password_str>]
execute backup config-with-forticlient-info ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config-with-forticlient-info tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup config-with-forticlient-info usb [<backup_password_str>]
execute backup config-with-forticlient-info usb-mode [<backup_password_str>]
execute backup full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup full-config usb <filename_str> [<backup_password_str>]
execute backup full-config usb-mode <filename_str> [<backup_password_str>]
execute backup ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute backup ipsuserdefsig tftp tftp <filename_str> <server_ipv4>
execute backup {disk | memory} alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]
```

```
execute backup {disk | memory} alllogs tftp <server_ipv4>
execute backup {disk | memory} alllogs usb
execute backup {disk | memory} log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_str> <password_str> {traffic | event | ids | virus | webfilter | spam | dlp | voip | app-ctrl | netscan}
execute backup {disk | memory} log tftp <server_ipv4> {traffic | event | ids | virus | webfilter | spam | dlp | voip | app-ctrl | netscan}
execute backup {disk | memory} log usb {traffic | event | ids | virus | webfilter | spam | dlp | voip | app-ctrl | netscan}
```

Variable	Description
config flash <comment>	Back up the system configuration to the flash disk. Optionally, include a comment.
config ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to an FTP server. Optionally, you can specify a password to protect the saved data.
config management-station <comment_str>	Back up the system configuration to a configured management station. If you are adding a comment, do not add spaces, underscore characters (_), or quotation marks (" ") or any other punctuation marks. The comment you enter displays in both the portal website and FortiGate web-based manager (System > Maintenance > Revision).
config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.
config usb <filename_str> [<backup_password_str>]	Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data.
config usb-mode [<backup_password_str>]	Back up the system configuration to a USB disk (Global admin only). Optionally, you can specify a password to protect the saved data.
config-with-forticlient-info ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to a file on an FTP server. Optionally, you can specify a password to protect the saved data.
config-with-forticlient-info tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.

Variable	Description
<code>config-with-forticlient-info usb [<backup_password_str>]</code>	Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data.
<code>config-with-forticlient-info usb-mode [<backup_password_str>]</code>	Back up the system configuration to a USB disk (Global admin only). Optionally, you can specify a password to protect the saved data.
<code>full-config ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]</code>	Back up the full system configuration to a file on an FTP server. You can optionally specify a password to protect the saved data.
<code>full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]</code>	Back up the full system configuration to a file on a TFTP server. You can optionally specify a password to protect the saved data.
<code>full-config usb <filename_str> [<backup_password_str>]</code>	Back up the full system configuration to a file on a USB disk. You can optionally specify a password to protect the saved data.
<code>full-config usb-mode <filename_str> [<backup_password_str>]</code>	Back up the full system configuration to a file on a USB disk (Global admin only). You can optionally specify a password to protect the saved data.
<code>ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]]</code>	Backup IPS user-defined signatures to a file on an FTP server.
<code>ipsuserdefsig tftp tftp <filename_str> <server_ipv4></code>	Back up IPS user-defined signatures to a file on a TFTP server.
<code>{disk memory} alllogs ftp <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>]</code>	Back up either all memory or all hard disk log files for this VDOM to an FTP server. The disk option is available on FortiGate models that log to a hard disk. The file name has the form: <log_file_name>_<VDOM>_<date>_<time>
<code>{disk memory} alllogs tftp <server_ipv4></code>	Back up either all memory or all hard disk log files for this VDOM to a TFTP server. The disk option is available on FortiGate models that log to a hard disk. The file name has the form: <log_file_name>_<VDOM>_<date>_<time>

Variable	Description
<code>{disk memory} alllogs usb</code>	Back up either all memory or all hard disk log files for this VDOM to a USB disk. The disk option is available on FortiGate models that log to a hard disk. The file name has the form: <code><log_file_name>_<VDOM>_<date>_<time></code>
<code>{disk memory} log ftp <server_ipv4[:port_int] server_fqdn[:port_int]> <username_str> <password_str> {traffic event ids virus webfilter spam dlp voip app-ctrl netscan}</code>	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiGate models that log to a hard disk.
<code>{disk memory} log tftp <server_ipv4> {traffic event ids virus webfilter spam dlp voip app-ctrl netscan}</code>	Back up the specified type of log file from either hard disk or memory to a TFTP server. The disk option is available on FortiGate models that log to a hard disk.
<code>{disk memory} log usb {traffic event ids virus webfilter spam dlp voip app-ctrl netscan}</code>	Back up the specified type of log file from either hard disk or memory to a USB disk. The disk option is available on FortiGate models that log to a hard disk.

Example

This example shows how to backup the FortiGate unit system configuration to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fgt.cfg 192.168.1.23
```

batch

Execute a series of CLI commands. `execute batch` commands are controlled by the Maintenance (`mntgrp`) access control group.

Syntax

```
execute batch [<cmd_cue>]
```

where `<cmd_cue>` is one of:

`end` — exit session and run the batch commands

`lastlog` — read the result of the last batch commands

`start` — start batch mode

`status` — batch mode status reporting if batch mode is running or stopped

Example

To start batch mode:

```
execute batch start
Enter batch mode...
```

To enter commands to run in batch mode:

```
config system global
  set refresh 5
end
```

To execute the batch commands:

```
execute batch end
Exit and run batch commands...
```

bypass-mode

Use this command to manually switch a FortiGate-600C or FortiGate-1000C into bypass mode. This is available in transparent mode only. If manually switched to bypass mode, the unit remains in bypass-mode until bypass mode is disabled.

Syntax

```
execute bypass-mode {enable | disable}
```

carrier-license

Use this command to enter a FortiOS Carrier license key if you have installed a FortiOS Carrier build on a FortiGate unit and need to enter a license key to enable FortiOS Carrier functionality.

Contact Fortinet Support for more information about this command.

Syntax

```
execute carrier-license <license_key>
```

Variable	Description
<license_key>	Enter the FortiOS Carrier license key supplied by Fortinet.

central-mgmt

Update Central Management Service account information. Also used receive configuration file updates from an attached FortiManager unit.

Syntax

```
execute central-mgmt set-mgmt-id <management_id>
```

```
execute central-mgmt register-device <fmg-serial-number> <fmg-register-password> <fgt-  
user-name> <fgt-password>  
execute central-mgmt unregister-device <fmg-serial-number>
```

`set-mgmt-id` is used to change or initially set the management ID, or your account number for Central Management Services. This account ID must be set for the service to be enabled.

`register-device` registers the FortiGate unit with a specific FortiManager unit specified by serial number. You must also specify the administrator name and password that the FortiManager unit uses to log on to the FortiGate unit.

`unregister-device` removes the FortiGate unit from the specified FortiManager unit's device list.

`update` is used to update your Central Management Service contract with your new management account ID. This command is to be used if there are any changes to your management service account.

Example

If you are registering with the Central Management Service for the first time, and your account number is 123456, you would enter the following:

```
execute central-mgmt set-mgmt-id 123456
```

cfg reload

Use this command to restore the saved configuration when the configuration change mode is `manual` or `revert`. This command has no effect if the mode is `automatic`, the default. The `set cfg-save` command in `system global` sets the configuration change mode.

When you reload the saved system configuration, the your session ends and the FortiGate unit restarts.

In the default configuration change mode, `automatic`, CLI commands become part of the saved unit configuration when you execute them by entering either `next` or `end`.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. You set the timeout in `system global` using the `set cfg-revert-timeout` command.

Syntax

```
execute cfg reload
```

Example

This is sample output from the command when successful:

```
# execute cfg reload  
configs reloaded. system will reboot.This is sample output from the command when not in  
runtime-only configuration mode:  
# execute cfg reload  
no config to be reloaded.
```

cfg save

Use this command to save configuration changes when the configuration change mode is `manual` or `revert`. If the mode is `automatic`, the default, all changes are added to the saved configuration as you make them and this command has no effect. The `set cfg-save` command in `system global` sets the configuration change mode.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are reverted automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. To change the timeout from the default of 600 seconds, go to `system global` and use the `set cfg-revert-timeout` command.

Syntax

```
execute cfg save
```

Example

This is sample output from the command:

```
# execute cfg save
config saved.
```

This is sample output when not in runtime-only configuration mode. It also occurs when in runtime-only configuration mode and no changes have been made:

```
# execute cfg save
no config to be saved.
```

clear system arp table

Clear all the entries in the arp table.

Syntax

```
execute clear system arp table
```

cli check-template-status

Reports the status of the secure copy protocol (SCP) script template.

Syntax

```
execute cli check-template-status
```

cli status-msg-only

Enable or disable displaying standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session. This command is used for compatibility with FortiManager.

Syntax

```
execute cli status-msg-only [enable | disable]
```

Variable	Description	Default
status-msg-only [enable disable]	Enable or disable standardized CLI error output messages. Entering the command without enable or disable disables displaying standardized output.	enable

client-reputation

Use these commands to retrieve or remove client reputation information.

Syntax

To erase all client reputation data

```
execute client-reputation erase
```

To retrieve client reputation host count

```
execute client-reputation host-count <rows>
```

To retrieve client reputation host details

```
execute client-reputation host detail <host>
```

To retrieve client reputation host summary

```
execute client-reputation host summary <host>
```

To purge old data

```
execute client-reputation purge
```

To view the top n records

```
execute client-reputation <n | all>
```

date

Get or set the system date.

Syntax

```
execute date [<date_str>]
date_str has the form yyyy-mm-dd, where
yyyy is the year and can be 2001 to 2037
mm is the month and can be 01 to 12
dd is the day of the month and can be 01 to 31
```

If you do not specify a date, the command returns the current system date. Shortened values, such as '06' instead of '2006' for the year or '1' instead of '01' for month or day, are not valid.

Example

This example sets the date to 17 September 2004:

```
execute date 2004-09-17
```

disk

Use this command to list and format hard disks installed in FortiGate units or individual partitions on these hard disks.

Syntax

```
execute disk format <partition1_ref_int> [...<partitionn_ref_int>]
execute disk list
execute disk scan <ref_int>
```

Variable	Description
format	Format the referenced disk partitions or disks. Separate reference numbers with spaces. If you enter a partition reference number the disk partition is formatted. If you enter a disk reference number the entire disk and all of its partitions are formatted.
list	List the disks and partitions and the reference number for each one.
scan	Scan a disk or partition and repair errors.
<ref_int>	Disk (device) or partition reference number.

The `execute disk format` command formats the specified partitions or disks and then reboots the system if a reboot is required.

In most cases you need to format the entire disk only if there is a problem with the partition. Formatting the partition removes all data from the partition. Formatting the disk removes all data from the entire disk and creates a single partition on the disk.

Examples

Use the following command to list the disks and partitions.

```
execute disk list
```

```
Disk Internal(boot) ref: 14.9GB type: SSD [ATA SanDisk SSD U100] dev: /dev/sda
partition ref: 3 14.4GB, 14.4GB free mounted: Y label: 7464A257123E07BB dev: /dev/sda3
```

In this example, there is only one partition and its reference number is 3.

Enter the following command to format the partition.

```
execute disk format 3
```

After a confirmation message the FortiGate unit formats the partition and restarts. This can take a few minutes.

disk raid

Use this command to view information about and change the raid settings on FortiGate units that support RAID.

Syntax

```
execute disk raid disable
execute disk raid enable {Raid-0 | Raid-1 | Raid-5}
execute disk raid rebuild
execute disk raid status
```

Variable	Description
disable	Disable raid for the FortiGate unit.
enable {Raid-0 Raid-1 Raid-5}	Change the RAID level on the FortiGate unit.
rebuild	Rebuild RAID on the FortiGate unit at the same RAID level. You can only execute this command if a RAID error has been detected. Changing the RAID level takes a while and deletes all data on the disk array.
status	Display information about the RAID disk array in the FortiGate unit.

Examples

Use the following command to display information about the RAID disk array in a FortiGate-82C.

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1000GB

Disk 1: OK Used 1000GB
Disk 2: OK Used 1000GB
Disk 3: OK Used 1000GB
Disk 4: Unavailable Not-Used 0GB
```

disk scan

Use this command to run a disk check operation.

Syntax

```
execute disk scan <ref_int>
```

where n is the partition "ref:" number for the disk, shown by `execute disk list`.

The operation requires the FortiGate unit to reboot. The command responds:

Example

```
# execute disk scan 3
scan requested for: 3/Internal (device=/dev/sda3)
This action requires the unit to reboot.
Do you want to continue? (y/n)
```

dhcp lease-clear

Clear all DHCP address leases.

Syntax

For IPv4:

```
execute dhcp lease-clear
```

For IPv6

```
execute dhcp6 lease-clear
```

dhcp lease-list

Display DHCP leases on a given interface

Syntax

For IPv4:

```
execute dhcp lease-list [interface_name]
```

For IPv6:

```
execute dhcp6 lease-list [interface_name]
```

If you specify an interface, the command lists only the leases issued on that interface. Otherwise, the list includes all leases issued by DHCP servers on the FortiGate unit.

If there are no DHCP leases in user on the FortiGate unit, an error will be returned.

disconnect-admin-session

Disconnect an administrator who is logged in.

Syntax

```
execute disconnect-admin-session <index_number>
```

To determine the index of the administrator that you want to disconnect, view the list of logged-in administrators by using the following command:

```
execute disconnect-admin-session ?
```

The list of logged-in administrators looks like this:

```
Connected:
INDEX  USERNAME  TYPE      FROM          TIME
0      admin     WEB       172.20.120.51 Mon Aug 14 12:57:23 2006
1      admin2    CLI       ssh(172.20.120.54) Mon Aug 14 12:57:23 2006
```

Example

This example shows how to disconnect the logged administrator `admin2` from the above list.

```
execute disconnect-admin-session 1
```

enter

Use this command to go from global commands to a specific virtual domain (VDM).

Only available when virtual domains are enabled and you are in config global.

After you enter the VDM, the prompt will not change from “(global)”. However you will be in the VDM with all the commands that are normally available in VDMs.

Syntax

```
execute enter <vdom>
```

Use “?” to see a list of available VDMs.

erase-disk

Use this command to reformat the boot device or an attached hard disk. Optionally, this command can restore the image from a TFTP server after erasing.

Syntax

```
execute erase-disk <disk_name>
```

The <disk_name> for the boot device is `boot`.

factoryreset

Reset the FortiGate configuration to factory default settings.

Syntax

```
execute factoryreset [keepvmlicense]
```

If `keepvmlicense` is specified (VM models only), the VM license is retained after reset.

Apart from the `keepvmlicense` option, this procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses.

factoryreset2

Reset the FortiGate configuration to factory default settings except VDOM and interface settings.

Syntax

```
execute factoryreset2 [keepvmlicense]
```

If `keepvmlicense` is specified (VM models only), the VM license is retained after reset.

formatlogdisk

Format the FortiGate hard disk to enhance performance for logging.

Syntax

```
execute formatlogdisk
```

In addition to deleting logs, this operation will erase all other data on the disk, including system configuration, quarantine files, and databases for antivirus and IPS.

forticarrier-license

Use this command to perform a FortiCarrier license upgrade.

Syntax

```
execute forticarrier-license <activation-code>
```

forticlient

Use these commands to manage FortiClient licensing.

Syntax

To view FortiClient license information

```
execute forticlient info
```

To show current FortiClient count

```
execute forticlient list <connection_type>  
where <connection_type> is one of:
```

0 - IPsec

1 - SSLVPN

2 - NAC (Endpoint Security)

3 - WAN optimization

4 - Test

To upgrade FortiClient licenses

```
execute forticlient upgrade <license_key_str>
```

FortiClient-NAC

Use the following command to load a FortiClient license onto a FortiGate unit.

Syntax

```
execute FortiClient-NAC update-registration-license <code>  
where <code> is the FortiClient registration license key/activation code.
```

fortiguard-log

Use this to manage FortiGuard Analysis and Management Service (FortiCloud) operation.

Syntax

To create a FortiCloud account

```
execute fortiguard-log create-account
```

To perform FortiCloud certification

```
execute fortiguard-log certification
```

To retrieve the FortiCloud agreement

```
execute fortiguard-log agreement
```

To test connection to a FortiCloud account

```
execute fortiguard-log try <account-id> <password>
```

To join FortiCloud

```
execute fortiguard-log join
```

To log in to a FortiCloud account

```
execute fortiguard-log login <account-id> <password>
```

To update the FortiGuard Analysis and Management Service contract

```
execute fortiguard-log update
```

fortitoken

Use these commands to activate and synchronize a FortiToken device. FortiToken devices are used in two-factor authentication of administrator and user account logons. The device generates a random six-digit code that you enter during the logon process along with user name and password.

Before they can be used to authenticate account logins, FortiToken devices must be activated with the FortiGuard service. When successfully activated, the status of the FortiToken device will change from New to Active.

Synchronization is sometimes needed due to the internal clock drift of the FortiToken device. It is not unusual for new FortiToken units to require synchronization before being put into service. Synchronization is accomplished by entering two sequential codes provided by the FortiToken.

Syntax

To activate one or more FortiToken devices

```
execute fortitoken activate <serial_number> [serial_number2 ... serial_numbern]
```

To import FortiToken OTP seeds

```
execute fortitoken import <seeds_file> <seeds_file_preshared_key>
```

To synchronize a FortiToken device

```
execute fortitoken sync <serial_number> <code> <next code>
```

To import a set of FortiToken serial numbers

```
execute fortitoken import-sn-file <ftk-sn>
```

FortiCare returns a set of 200 serial numbers that are in the same serial number range as the specified FortiToken device.

fortitoken-mobile

Use these commands to activate and synchronize a FortiToken Mobile card. FortiToken Mobile cards are used in two-factor authentication of administrator and user account logons. The FortiGate unit sends a random six-digit code to the mobile device by email or SMS that the user enters during the logon process along with user name and password.

Syntax

To import the FortiToken Mobile card serial number

```
execute fortitoken-mobile import <activation_code>
```

To poll a FortiToken Mobile token state

```
execute fortitoken-mobile poll
```

To provision a FortiToken Mobile token

```
execute fortitoken-mobile provision <token_serial_number>
```

fssso refresh

Use this command to manually refresh user group information from Directory Service servers connected to the FortiGate unit using the Fortinet Single Sign On (FSSO) agent.

Syntax

```
execute fssso refresh
```

ha disconnect

Use this command to disconnect a FortiGate unit from a functioning cluster. You must specify the serial number of the unit to be disconnected. You must also specify an interface name and assign an IP address and netmask to this interface of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

To disconnect the unit from the cluster, the `execute ha disconnect` command sets the HA mode of the disconnected unit to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0. The interface specified in the command is set to the IP address and netmask that you specify in the command. In addition all management access to this interface is enabled. Once the FortiGate unit is disconnected you can use SSH, telnet, HTTPS, or HTTP to connect to and manage the FortiGate unit.

Syntax

```
execute ha disconnect <cluster-member-serial_str> <interface_str> <address_ipv4>  
                   <address_ipv4mask>
```

Variable	Description
cluster-member-serial_str	The serial number of the cluster unit to be disconnected.
interface_str	The name of the interface to configure. The command configures the IP address and netmask for this interface and also enables all management access for this interface.

Example

This example shows how to disconnect a cluster unit with serial number FGT5002803033050. The internal interface of the disconnected unit is set to IP address 1.1.1.1 and netmask 255.255.255.0.

```
execute ha disconnect FGT5002803033050 internal 1.1.1.1 255.255.255.0
```

ha ignore-hardware-revision

Use this command to set ignore-hardware-revision status.

Syntax

To view ignore-hardware-revision status

```
execute ha ignore-hardware-revision status
```

To set ignore-hardware-revision status

```
execute ha ignore-hardware-revision {enable | disable}
```

ha manage

Use this command from the CLI of a FortiGate unit in an HA cluster to log into the CLI of another unit in the cluster. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

You can use CLI commands to manage the cluster unit that you have logged into. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.

Syntax

```
execute ha manage <cluster-index>
```

Variable	Description
cluster-index	<p>The cluster index is assigned by the FortiGate Clustering Protocol according to cluster unit serial number. The cluster unit with the highest serial number has a cluster index of 0. The cluster unit with the second highest serial number has a cluster index of 1 and so on.</p> <p>Enter ? to list the cluster indexes of the cluster units that you can log into. The list does not show the unit that you are already logged into.</p>

Example

This example shows how to log into a subordinate unit in a cluster of three FortiGate units. In this example you have already logged into the primary unit. The primary unit has serial number FGT308210300056. The subordinate units have serial numbers FGT3012803021709 and FGT3082103021989.

```
execute ha manage ?
<id>   please input slave cluster index.
<0>    Subsidiary unit FGT3012803021709
<1>    Subsidiary unit FGT3082103021989
```

Type 0 and press enter to connect to the subordinate unit with serial number FGT3012803021709 and log in with a valid administrator account. The CLI prompt changes to the host name of this unit. To return to the primary unit, type `exit`.

From the subordinate unit you can also use the `execute ha manage` command to log into the primary unit or into another subordinate unit. Enter the following command:

```
execute ha manage ?
<id>   please input slave cluster index.
<1>    Subsidiary unit FGT3082103021989
<2>    Subsidiary unit FGT308210300056
```

Type 2 and press enter to log into the primary unit or type 1 and press enter to log into the other subordinate unit with a valid administrator account. The CLI prompt changes to the host name of this unit.

ha synchronize

Use this command from a subordinate unit in an HA cluster to manually synchronize its configuration with the primary unit or to stop a synchronization process that is in progress.

Syntax

```
execute ha synchronize {start | stop}
```

Variable	Description
start	Start synchronizing the cluster configuration.
stop	Stop the cluster from completing synchronizing its configuration.

interface dhcpclient-renew

Renew the DHCP client for the specified DHCP interface and close the CLI session. If there is no DHCP connection on the specified port, there is no output.

Syntax

```
execute interface dhcpclient-renew <port>
```

Example

This is the output for renewing the DHCP client on port1 before the session closes:

```
# execute interface dhcpclient-renew port1
renewing dhcp lease on port1
```

interface pppoe-reconnect

Reconnect to the PPPoE service on the specified PPPoE interface and close the CLI session. If there is no PPPoE connection on the specified port, there is no output.

Syntax

```
execute interface pppoe-reconnect <port>
```

log backup

Use this command to back up all logs, index files, and report databases. The files are compressed and combined into a TAR archive.

Syntax

```
execute log backup <file name>
where <file name> is the name of the backup file to create.
```

log client-reputation-report

Use these commands to control client-reputation log actions.

Syntax

To accept a host so that it has its own baselines

```
execute log client-reputation-report accept <policy-id> <host>
```

To clear all auto-profile data

```
execute log client-reputation-report clear
```

To ignore a host, removing it from the abnormal list

```
execute log client-reputation-report ignore <policy-id> <host>
```

To refresh the data of one option result

```
execute log client-reputation-report refresh <policy-id> <option> <action>
```

<option> is one of bandwidth, session, failconn, geo, or app

<action> is one of data, baseline, or data_baseline (both data and baseline)

To get baseline/average information of one option

```
execute log client-reputation-report result baseline <policy-id> <option>
```

<option> is one of bandwidth, session, or failconn

To get hourly data of a host visiting a country or using an application

```
execute log client-reputation-report result details {hourly | total} <policy-id>
    <option> <name> <host>
```

<option> is geo or app

<name> is the name of the country or application

To list abnormal hosts of one or all options

```
execute log client-reputation-report result list <policy-id> <option>
```

<option> is geo, app, or all

To list periodical data of one host of one option

```
execute log client-reputation-report result period <policy-id> <option> <host>
    <periods>
```

<option> is one of bandwidth, session, failconn, geo, or app

<periods> is number of periods to list

To list the top 10 abnormal hosts of one option

```
execute log client-reputation-report result top10 <policy-id> <option>
```

<option> is one of bandwidth, session, failconn, geo, or app

To run reports immediately

```
execute log client-reputation-report run <policy-id>
```


log convert-oldlogs

Use this command to convert old compact logs to the new format. This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

Syntax

```
execute log convert-oldlogs
```

log delete-all

Use this command to clear all log entries for this VDOM in memory and current log files on hard disk. If your FortiGate unit has no hard disk, only log entries in system memory will be cleared. You will be prompted to confirm the command.

Syntax

```
execute log delete-all
```

log delete-oldlogs

Use this command to delete old compact logs. This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

Syntax

```
execute log delete-oldlogs
```

log detail

Display UTM-related log entries for traffic log entries in this VDOM.

Syntax

```
execute log detail <category> <utm-ref>
```

where <category> is one of:

- 2: utm-virus
- 3: utm-webfilter
- 4: utm-ips
- 5: utm-spam
- 9: utm-dlp
- 10: utm-app-ctrl

You can obtain `<utm-ref>` from the `execute log display` output.

log display

Use this command to display log messages for this VDOM that you have selected with the `execute log filter` command.

Syntax

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start-line 1
execute log display
```

You can restore the log filters to their default values using the command

```
execute log filter reset
```

log downgrade-log

Use this command to downgrade existing logs to v5.0 format prior to a firmware downgrade to FortiOS v5.0.

Syntax

```
execute log downgrade-log
```

log filter

Use this command to select log messages in this VDOM for viewing or deletion. You can view one log category on one device at a time. Optionally, you can filter the messages to select only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Commands are cumulative. If you omit a required variable, the command displays the current setting.

Use as many `execute log filter` commands as you need to define the log messages that you want to view.

Syntax

```
execute log filter category <category_name>
execute log filter device {disk | memory}
execute log filter dump
execute log filter field <name> <value> [<value2>,...<valuen>] [not]
execute log filter ha-member <unitsn_str>
execute log filter reset [all | field]
execute log filter rolled_number <number>
execute log filter sortby <field> [max-sort-lines]
execute log filter start-line <line_number>
```

```
execute log filter view-lines <count>
```

Variable	Description	Default
category <category_name>	Enter the type of log you want to select. To see a list of available categories, enter <code>execute log filter category</code>	event
device {disk memory}	Device where the logs are stored.	disk
dump	Display current filter settings.	No default.
field <name> <value> [<value2>,...<value n>] [not]	Enter <code>execute log filter field</code> to view the list of field names. Press Enter after <name> to view information about value parameters for that field. <code>not</code> inverts the field value condition.	No default.
ha-member <unitsn_str>	Select logs from the specified HA cluster member. Enter the serial number of the unit.	
reset [all field]	Execute this command to reset all filter settings. You can use field option to reset only filter field settings.	No default.
rolled_number <number>	Select logs from rolled log file. 0 selects current log file.	0
sortby <field> [max-sort-lines]	Sort logs by specified field.	No default.
start-line <line_ number>	Select logs starting at specified line number.	1
view-lines <count>	Set lines per view. Range: 5 to 1000	10

log fortianalyzer test-connectivity

Use this command to test the connection to the FortiAnalyzer unit. This command is available only when FortiAnalyzer is configured.

Syntax

```
execute log fortianalyzer test-connectivity
```

Example

When FortiAnalyzer is connected, the output looks like this:

```
FortiAnalyzer Host Name: FortiAnalyzer-800B
```

```
FortiGate Device ID: FG50B3G06500085
Registration: registered
Connection: allow
Disk Space (Used/Allocated): 468/1003 MB
Total Free Space: 467088 MB
Log: Tx & Rx
Report: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

When FortiAnalyzer is not connected, the output is: `Connect Error`

log list

You can view the list of current and rolled log files for this VDOM on the console. The list shows the file name, size and timestamp.

Syntax

```
execute log list <category>
```

To see a list of available categories, enter

```
execute log list
```

Example

The output looks like this:

```
elog 8704 Fri March 6 14:24:35 2009
elog.1 1536 Thu March 5 18:02:51 2009
elog.2 35840 Wed March 4 22:22:47 2009
```

At the end of the list, the total number of files in the category is displayed. For example:

```
501 event log file(s) found.
```

log rebuild-sqldb

Use this command to rebuild the SQL database from log files.

If run in the VDOM context, only this VDOM's SQL database is rebuilt. If run in the global context, the SQL database is rebuilt for all VDOMs.

If SQL logging is disabled, this command is unavailable.

Syntax

```
execute log rebuild-sqldb
```

log recreate-sqldb

Use this command to recreate SQL log database.

If SQL logging is disabled, this command is unavailable.

Syntax

```
execute log recreate-sqlldb
```

log-report reset

Use this command to delete all logs, archives and user configured report templates.

Syntax

```
execute log-report reset
```

log restore

Use this command to restore up all logs, index files, and report databases from a backup file created with the "[log backup](#)" on page 1071 command.

This command will wipe out all existing logs and report database for the vdom. It is only available for debug firmware builds.

It is recommended to kill reportd and miglogd prior to running this command.

```
kill -3 1
killall miglogd
killall reportd
```

Syntax

```
execute log restore <file name>
```

where <file name> is the name of the backup file to use.

log roll

Use this command to roll all log files.

Syntax

```
execute log roll
```

log shift-time

Use this command in conjunction with the "[log backup](#)" on page 1071 and "[log restore](#)" on page 1077 commands. You can load a log set generated previously to do demos or testing without needing to regenerate data.

Syntax

```
execute log shift-time <number of hours>
```

log upload-progress

Use this command to display the progress of the latest log upload.

Syntax

```
execute log upload-progress
```

modem dial

Dial the modem.

The dial command dials the accounts configured in `config system modem` until it makes a connection or it has made the maximum configured number of redial attempts.

This command can be used if the modem is in Standalone mode.

Syntax

```
execute modem dial
```

modem hangup

Hang up the modem.

This command can be used if the modem is in Standalone mode.

Syntax

```
execute modem hangup
```

modem trigger

This command sends a signal to the modem daemon, which causes the state machine to re-evaluate its current state. If for some reason the modem should be connected but isn't, then it will trigger a redial. If the modem should not be connected but is, this command will cause the modem to disconnect.

Syntax

```
execute modem trigger
```

mrouter clear

Clear multicast routes, RP-sets, IGMP membership records or routing statistics.

Syntax

Clear IGMP memberships:

```
execute mrouter clear igmp-group {{<group-address>} <interface-name>}
execute mrouter clear igmp-interface <interface-name>
```

Clear multicast routes:

```
execute mrouter clear <route-type> {<group-address> {<source-address>}}
```

Clear PIM-SM RP-sets learned from the bootstrap router (BSR):

```
execute mrouter clear sparse-mode-bsr
```

Clear statistics:

```
execute mrouter clear statistics {<group-address> {<source-address>}}
```

Variable	Description
<interface-name>	Enter the name of the interface on which you want to clear IGMP memberships.
<group-address>	Optionally enter a group address to limit the command to a particular group.
<route-type>	Enter one of: dense-routes - clear only PIM dense routes multicast-routes - clear all types of multicast routes sparse-routes - clear only sparse routes
<source-address>	Optionally, enter a source address to limit the command to a particular source address. You must also specify group-address.

netscan

Use this command to start and stop the network vulnerability scanner and perform related functions.

Syntax

```
execute netscan import
execute netscan list
execute netscan start scan
execute netscan status
execute netscan stop
```

Variable	Description
import	Import hosts discovered on the last asset discovery scan.
list	List the hosts discovered on the last asset discover scan.
start scan	Start configured vulnerability scan.
status	Display the status of the current network vulnerability scan.
stop	Stop the current network vulnerability scan.

pbx

Use this command to view active channels and to delete, list or upload music files for when music is playing while a caller is on hold.

Syntax

```
execute pbx active-call <list>
execute pbx extension <list>
execute pbx ftgd-voice-pkg {sip-trunk}
execute pbx music-on-hold {delete | list | upload}
execute pbx prompt upload ftp <file.tgz> <ftp_server_address>[:port] [<username>]
[password]
execute pbx prompt upload tftp <file.tgz> <ftp_server_address>[:port] [<username>]
[password]
execute pbx prompt upload usb <file.tgz> <ftp_server_address>[:port] [<username>]
[password]
execute pbx restore-default-prompts
execute pbx sip-trunk list
```

Variables	Description
active-call <list>	Enter to display a list of the active calls being processed by the FortiGate Voice unit.
extension <list>	Enter to display the status of all extensions with SIP phones that have connected to the FortiGate Voice unit.
ftgd-voice-pkg {sip-trunk}	Enter to retrieve FortiGuard voice package sip trunk information.
music-on-hold {delete list upload}	Enter to either delete, list or upload music on hold files. You can upload music on hold files using FTP, TFTP, or from a USB drive plugged into the FortiGate Voice unit.

Variables	Description
prompt upload ftp <file.tgz> <ftp_ server_address> [:port] [<username>] [password>]	Upload new pbx voice prompt files using FTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename, FTP server address (domain name of IPv4 address) and if required the username and password for the server.
prompt upload tftp <file.tgz> <tftp_ server_address> [:port] [<username>] [password>]	Upload new pbx voice prompt files using TFTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename and TFTP server IP address.
prompt upload usb <file.tgz> <tftp_ server_address> [:port] [<username>] [password>]	Upload new pbx voice prompt files from a USB drive plugged into the FortiGate Voice unit. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename.
restore-default-prompts	Restore default English voicemail and other PBX system prompts. Use this command if you have changed the default prompts and want to restore the default settings.
sip-trunk list	Enter to display the status of all SIP trunks that have been added to the FortiGate Voice configuration.

Example command output

Enter the following command to view active calls:

```
execute pbx active-call

Call-From    Call-To    Durationed
6016         6006      00:00:46
```

Enter the following command to display the status of all extensions

```
execute pbx extension list
Extension Host Dialplan
6052 Unregister company-default
6051 Unregister company-default
6050 Unregister company-default
6022 Unregister company-default
6021/6021 172.30.63.34 company-default
6020 Unregister company-default
```

Enter the following command to display the status of all SIP trunks

```
execute pbx sip-trunk list
Name      Host      Username      Account-Type  State
Provider_1 192.169.20.1 +5555555      Static        N/A
```

ping

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and another network device.

Syntax

```
execute ping {<address_ipv4> | <host-name_str>}
<host-name_str> should be an IP address, or a fully qualified domain name.
```

Example

This example shows how to ping a host with the IP address 172.20.120.16.

```
#execute ping 172.20.120.16

PING 172.20.120.16 (172.20.120.16): 56 data bytes
64 bytes from 172.20.120.16: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.20.120.16: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.20.120.16 ping statistics ---
 5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

ping-options, ping6-options

Set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiGate unit and another network device.

Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
data-size <bytes>	Specify the datagram size in bytes.	56

Variable	Description	Default
df-bit {yes no}	Set <code>df-bit</code> to <code>yes</code> to prevent the ICMP packet from being fragmented. Set <code>df-bit</code> to <code>no</code> to allow the ICMP packet to be fragmented.	no
pattern <2-byte_hex>	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the <code>data_size</code> parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default.
repeat-count <repeats>	Specify how many times to repeat ping.	5
source {auto <source-intf_ip>}	Specify the FortiGate interface from which to send the ping. If you specify <code>auto</code> , the FortiGate unit selects the source address and interface based on the route to the <code><host-name_str></code> or <code><host_ip></code> . Specifying the IP address of a FortiGate interface tests connections to different network segments from the specified interface.	auto
timeout <seconds>	Specify, in seconds, how long to wait until ping times out.	2
tos <service_type>	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted. lowdelay = minimize delay throughput = maximize throughput reliability = maximize reliability lowcost = minimize cost	0
ttl <hops>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes no}	Select <code>yes</code> to validate reply data.	no
view-settings	Display the current ping-option settings.	No default.

Example

Use the following command to increase the number of pings sent.

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiGate interface with IP address 192.168.10.23.

```
execute ping-options source 192.168.10.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and an IPv6 capable network device.

Syntax

```
execute ping6 {<address_ipv6> | <host-name_str>}
```

Example

This example shows how to ping a host with the IPv6 address 12AB:0:0:CD30:123:4567:89AB:CDEF.

```
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

policy-packet-capture delete-all

Use this command to delete captured packets.

Syntax

```
execute policy-packet-capture delete-all
```

You will be asked to confirm that you want delete the packets.

reboot

Restart the FortiGate unit.

Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute reboot <comment "comment_string">
```

<comment "comment_string"> allows you to optionally add a message that will appear in the hard disk log indicating the reason for the reboot. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute reboot comment "December monthly maintenance"
```

report

Use these commands to manage reports.

Syntax

To flash report caches:

```
execute report flash-cache
```

To recreate the report database:

```
execute report recreate-db
```

To generate a report:

```
execute report run [<layout_name>["start-time" "end-time"]]
```

The start and end times have the format yyyy-mm-dd hh:mm:ss

report-config reset

Use this command to reset report templates to the factory default. Logs are not deleted.

If SQL logging is disabled, this command is unavailable.

Syntax

```
execute report-config reset
```

restore

Use this command to

- restore the configuration from a file
- change the FortiGate firmware
- change the FortiGate backup firmware
- restore an IPS custom signature file

When virtual domain configuration is enabled (in `system global`, `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin account can restore the configuration from this file.

A backup file from a regular administrator account contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```

execute restore av ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore av tftp <filename_str> <server_ipv4[:port_int]>
execute restore config flash <revision>
execute restore config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_
int]> [<username_str> <password_str>] [<backup_password_str>]
execute restore config management-station {normal | template | script} <rev_int>
execute restore config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute restore config usb <filename_str> [<backup_password_str>]
execute restore config usb-mode [<backup_password_str>]
execute restore forticlient tftp <filename_str> <server_ipv4>
execute restore image flash <revision>
execute restore image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_
int]> [<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
execute restore image usb <filename_str>
execute restore ips ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_
int]> [<username_str> <password_str>]
execute restore ips tftp <filename_str> <server_ipv4>
execute restore ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] | server_fqdn
[:port_int]> [<username_str> <password_str>]
execute restore ipsuserdefsig tftp <filename_str> <server_ipv4>
execute restore secondary-image ftp <filename_str> <server_ipv4[:port_int] | server_
fqdn[:port_int]> [<username_str> <password_str>]
execute restore secondary-image tftp <filename_str> <server_ipv4>
execute restore secondary-image usb <filename_str>
execute restore src-vis <src-vis-pkgfile>
execute restore vcm {ftp | tftp} <filename_str> <server_ipv4>
execute restore vmlicense {ftp | tftp} <filename_str> <server_ipv4>

```

Variable	Description
av ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>]	Download the antivirus database file from an FTP server to the FortiGate unit.
av tftp <filename_str> <server_ipv4[:port_int]>	Download the antivirus database file from a TFTP server to the FortiGate unit.
config flash <revision>	Restore the specified revision of the system configuration from the flash disk.

Variable	Description
<pre>config ftp <filename_str> <server_ipv4[:port_ int] server_fqdn [:port_int]> [<username_str> <password_str>] [<backup_ password_str>]</pre>	<p>Restore the system configuration from an FTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config management- station {normal template script} <rev_int></pre>	<p>Restore the system configuration from the central management server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p><code>rev_int</code> is the revision number of the saved configuration to restore. Enter 0 for the most recent revision.</p>
<pre>config tftp <filename_str> <server_ipv4> [<backup_ password_str>]</pre>	<p>Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config usb <filename_str> [<backup_ password_str>]</pre>	<p>Restore the system configuration from a file on a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config usb-mode [<backup_ password_str>]</pre>	<p>Restore the system configuration from a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords. When the USB drive is removed, the FortiGate unit needs to reboot and revert to the unit's existing configuration.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>forticlient tftp <filename_str> <server_ipv4></pre>	<p>Download the FortiClient image from a TFTP server to the FortiGate unit. The filename must have the format: <code>FortiClientSetup_<versionmajor>.<versionminor>.<build>.exe</code>. For example, <code>FortiClientSetup.4.0.377.exe</code>.</p>
<pre>image flash <revision></pre>	<p>Restore specified firmware image from flash disk.</p>

Variable	Description
<pre>image ftp <filename_str> <server_ipv4[:port_ int] server_fqdn [:port_int]> [<username_str> <password_str>]</pre>	<p>Download a firmware image from an FTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.</p> <p>This command is not available in multiple VDOM mode.</p>
<pre>image management- station <version_ int></pre>	<p>Download a firmware image from the central management station. This is available if you have configured a FortiManager unit as a central management server. This is also available if your account with FortiGuard Analysis and Management Service allows you to upload firmware images.</p>
<pre>image tftp <filename_str> <server_ipv4></pre>	<p>Download a firmware image from a TFTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.</p> <p>This command is not available in multiple VDOM mode.</p>
<pre>image usb <filename_str></pre>	<p>Download a firmware image from a USB disk to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.</p>
<pre>ips ftp <filename_ str> <server_ipv4 [:port_int] server_ fqdn[:port_int]> [<username_str> <password_str>]</pre>	<p>Download the IPS database file from an FTP server to the FortiGate unit.</p>
<pre>ips tftp <filename_ str> <server_ipv4></pre>	<p>Download the IPS database file from a TFTP server to the FortiGate unit.</p>
<pre>ipsuserdefsig ftp <filename_str> <server_ipv4[:port_ int] server_fqdn [:port_int]> [<username_str> <password_str>]</pre>	<p>Restore IPS custom signature file from an FTP server. The file will overwrite the existing IPS custom signature file.</p>
<pre>ipsuserdefsig tftp <filename_str> <server_ipv4></pre>	<p>Restore an IPS custom signature file from a TFTP server. The file will overwrite the existing IPS custom signature file.</p>

Variable	Description
secondary-image ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>]	Download a firmware image from an FTP server as the backup firmware of the FortiGate unit. Available on models that support backup firmware images.
secondary-image tftp <filename_str> <server_ipv4>	Download a firmware image from a TFTP server as the backup firmware of the FortiGate unit. Available on models that support backup firmware images.
secondary-image usb <filename_str>	Download a firmware image from a USB disk as the backup firmware of the FortiGate unit. The unit restarts when the upload is complete. Available on models that support backup firmware images.
src-vis <src-vis-pkgfile>	Download source visibility signature package.
vcm {ftp tftp} <filename_str> <server_ipv4>	Restore VCM engine/plugin from an ftp or tftp server.
vmlicense {ftp tftp} <filename_str> <server_ipv4>	Restore VM license (VM version of product only).

Example

This example shows how to upload a configuration file from a TFTP server to the FortiGate unit and restart the FortiGate unit with this configuration. The name of the configuration file on the TFTP server is `backupconfig`. The IP address of the TFTP server is 192.168.1.23.

```
execute restore config tftp backupconfig 192.168.1.23
```

revision

Use these commands to manage configuration and firmware image files on the local disk.

Syntax

To delete a configuration file

```
execute revision delete config <revision>
```

To delete a firmware image file

```
execute revision delete image <revision>
```

To list the configuration files

```
execute revision list config
```

To delete a firmware image file

```
execute revision list image
```

router clear bfd session

Use this command to clear bi-directional forwarding session.

Syntax

```
execute router clear bfd session <src_ip> <dst_ip> <interface>
```

Variable	Description
<src_ip>	Select the source IP address of the session.
<dst_ip>	Select the destination IP address of the session.
<interface>	Select the interface for the session.

router clear bgp

Use this command to clear BGP peer connections.

Syntax

```
execute router clear bgp all [soft] [in | out]
execute router clear bgp as <as_number> [soft] [in | out]
execute router clear bgp dampening {ip_address | ip/netmask}
execute router clear bgp external {in prefix-filter} [soft] [in | out]
execute router clear bgp flap-statistics {ip_address | ip/netmask}
execute router clear bgp ip <ip_address> [soft] [in | out]
```

Variable	Description
all	Clear all BGP peer connections.
as <as_number>	Clear BGP peer connections by AS number.
dampening {ip_address ip/netmask}	Clear route flap dampening information for peer or network.
external {in prefix-filter}	Clear all external peers.

Variable	Description
ip <ip_address>	Clear BGP peer connections by IP address.
peer-group	Clear all members of a BGP peer-group.
[in out]	Optionally limit clear operation to inbound only or outbound only.
flap-statistics {ip_address ip/netmask}	Clear flap statistics for peer or network.
soft	Do a soft reset that changes the configuration but does not disturb existing sessions.

router clear ospf process

Use this command to clear and restart the OSPF router.

Syntax

IPv4:

```
execute router clear ospf process
```

IPv6:

```
execute router clear ospf6 process
```

router restart

Use this command to restart the routing software.

Syntax

```
execute router restart
```

send-fds-statistics

Use this command to send an FDS statistics report now, without waiting for the FDS statistics report interval to expire.

Syntax

```
execute send-fds-statistics
```

sensor detail

Use this command to provide information on the FortiGate's hardware components. This command is only supported on select FortiGate models. For example, it does not work on the 100D or the 200D but it does work on the 500D and the 900D.

Syntax

```
execute sensor detail
```

If you have VDOMs configured on your FortiGate, enter:

```
config global
  execute sensor detail
end
```

Example

```
# execute sensor detail
1 +3.3V alarm=0 value=3.3342 threshold_status=0
  type=2/1
  upper_non_recoverable=3.6906
  upper_critical=3.6258
  upper_non_critical=3.5124
  lower_non_critical=3.0912
  lower_critical=2.994
  lower_non_recoverable=2.9292
2 +5V alarm=0 value=5.0725 threshold_status=0
  type=2/1
  upper_non_recoverable=5.587
  upper_critical=5.489
  upper_non_critical=5.342
  lower_non_critical=4.6805
  lower_critical=4.5335
  lower_non_recoverable=4.4355
3 +12V alarm=0 value=12.195 threshold_status=0
  type=2/1
  upper_non_recoverable=14.083
  upper_critical=13.729
  upper_non_critical=13.434
  lower_non_critical=10.602
  lower_critical=10.366
  lower_non_recoverable=10.012
. . .
```

sensor list

Use this command to provide information on the FortiGate's hardware components. This command is only supported on select FortiGate models. For example, it does not work on the 100D or the 200D but it does work on the 500D and the 900D.

Syntax

```
execute sensor list
```

If you have VDOMs configured on your FortiGate, enter:

```
config global
  execute sensor list
end
```

Example

```
# execute sensor list
1 +3.3V alarm=0 value=3.2856 threshold_status=0
2 +5V alarm=0 value=5.0235 threshold_status=0
3 +12V alarm=0 value=12.136 threshold_status=0
4 CPU VCCP alarm=0 value=0.9609 threshold_status=0
5 CPU VTT alarm=0 value=1.0589 threshold_status=0
6 CPU PVSA alarm=0 value=0.9315 threshold_status=0
7 P1V8 alarm=0 value=1.7841 threshold_status=0
8 P1V5 alarm=0 value=1.4999 threshold_status=0
9 PCH +1.05V alarm=0 value=1.04 threshold_status=0
10 VCC 2V5 alarm=0 value=2.432 threshold_status=0
11 MAIN 12V alarm=0 value=11.904 threshold_status=0
12 VCC 1V15 alarm=0 value=1.136 threshold_status=0
13 DDR3 VTT alarm=0 value=0.736 threshold_status=0
14 RPS 12V alarm=1 value=0 threshold_status=0x7
15 NCT +3.3V alarm=0 value=3.216 threshold_status=0
16 NCT VBAT alarm=0 value=3.264 threshold_status=0
17 NCT +3.3VSB alarm=0 value=3.216 threshold_status=0
18 NCT VTT alarm=0 value=1.04 threshold_status=0
19 DTS CPU alarm=0 value=50 threshold_status=0
20 CPU Core 0 alarm=0 value=49 threshold_status=0
21 CPU Core 1 alarm=0 value=50 threshold_status=0
22 TD1 alarm=0 value=37 threshold_status=0
23 TD2 alarm=0 value=25 threshold_status=0
24 FAN_TMP_3 alarm=0 value=35 threshold_status=0
25 LM75 U72 alarm=0 value=28 threshold_status=0
26 LM75 U65 alarm=0 value=31 threshold_status=0
27 LM75 U62 alarm=0 value=32 threshold_status=0
28 FAN1 alarm=0 value=4900 threshold_status=0
29 FAN2 alarm=0 value=5000 threshold_status=0
30 FAN3 alarm=0 value=4700 threshold_status=0
```

set system session filter

Use these commands to define the session filter for `get system session` commands.

Syntax

To clear the filter settings

```
execute set system session filter clear
  {all|dport|dst|duration|expire|policy|proto|sport|src|vd}
```

To specify destination port

```
execute set system session filter dport <port_range>
```

To specify destination IP address

```
execute set system session filter dst <ip_range>
```

To specify duration

```
execute set system session filter duration <duration_range>
```

To specify expiry

```
execute set system session filter expire <expire_range>
```

To list the filter settings

```
execute set system session filter list
```

To invert a filter setting

```
execute set system session filter negate  
{dport|dst|duration|expire|policy|proto|sport|src|vd}
```

To specify firewall policy ID

```
execute set system session filter policy <policy_range>
```

To specify protocol

```
execute set system session filter proto <protocol_range>
```

To specify source port

```
execute set system session filter sport <port_range>
```

To specify source IP address

```
execute set system session filter src <ip_range>
```

To specify virtual domain

```
execute set system session filter vd <vdom_index>
```

Variable	Description
<duration_range>	The start and end times, separated by a space.
<expire_range>	The start and end times, separated by a space.
<ip_range>	The start and end IP addresses, separated by a space.
<policy_range>	The start and end policy numbers, separated by a space.

Variable	Description
<port_range>	The start and end port numbers, separated by a space.
<protocol_range>	The start and end protocol numbers, separated by a space.
<vdom_index>	The VDOM index number. -1 means all VDOMs.

set-next-reboot

Use this command to start the FortiGate unit with primary or secondary firmware after the next reboot. Available on models that can store two firmware images. By default, the FortiGate unit loads the firmware from the primary partition.

VDOM administrators do not have permission to run this command. It must be executed by a super administrator.

Syntax

```
execute set-next-reboot {primary | secondary}
```

sfp-mode-sgmii

Change the SFP mode for an NP2 card to SGMII. By default when an AMC card is inserted the SFP mode is set to SERDES mode by default.

If a configured NP2 card is removed and re-inserted, the SFP mode goes back to the default.

In these situations, the `sfpmode-sgmii` command will change the SFP mode from SERDES to SGMII for the interface specified.

Syntax

```
execute sfpmode-sgmii <interface>
```

<interface> is the NP2 interface where you are changing the SFP mode.

shutdown

Shut down the FortiGate unit now. You will be prompted to confirm this command.

Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute shutdown [comment <comment_string>]
```

`comment` is optional but you can use it to add a message that will appear in the event log message that records the shutdown. The `comment` message of the does not appear on the Alert Message console. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute shutdown comment "emergency facility shutdown"
```

An event log message similar to the following is recorded:

```
2009-09-08 11:12:31 critical admin 41986 ssh(172.20.120.11) shutdown User admin shutdown
the device from ssh(172.20.120.11). The reason is 'emergency facility shutdown'
```

ssh

Use this command to establish an ssh session with another system.

Syntax

```
execute ssh <destination> [<port>]
<destination> - the destination in the form user@ip or user@host.
[<port>] - optional TCP port number
```

Example

```
execute ssh admin@172.20.120.122
To end an ssh session, type exit:
FGT-6028030112 # exit
Connection to 172.20.120.122 closed.
FGT-8002805000 #
```

sync-session

Use this command to force a session synchronization.

Syntax

```
execute sync-session
```

system custom-language import

Use this command to import a custom language file from a TFTP server.

The web-based manager provides a downloadable template file. Go to *System > Config > Advanced*.

Syntax

```
execute system custom-language import <lang_name> <file_name> <tftp_server_ip>
```


<lang_name> - language name

<file_name> - the language file name

<tftp_server_ip> the TFTP server IP address

system fortisandbox test-connectivity

Use this command to query FortiSandbox connection status.

Syntax

```
execute system fortisandbox test-connectivity
```

tac report

Use this command to create a debug report to send to Fortinet Support. Normally you would only use this command if requested to by Fortinet Support.

Syntax

```
execute tac report
```

telnet

Use telnet client. You can use this tool to test network connectivity.

Syntax

```
execute telnet <telnet_ipv4>  
<telnet_ipv4> is the address to connect with.
```

Type `exit` to close the telnet session.

time

Get or set the system time.

Syntax

```
execute time [<time_str>  
time_str has the form hh:mm:ss, where  
hh is the hour and can be 00 to 23  
mm is the minutes and can be 00 to 59  
ss is the seconds and can be 00 to 59
```

If you do not specify a time, the command returns the current system time.

You are allowed to shorten numbers to only one digit when setting the time. For example both 01:01:01 and 1:1:1 are allowed.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

traceroute

Test the connection between the FortiGate unit and another network device, and display information about the network hops between the device and the FortiGate unit.

Syntax

```
execute traceroute {<ip_address> | <host-name>}
```

Example

This example shows how to test the connection with <http://docs.forticare.com>. In this example the traceroute command times out after the first hop indicating a possible problem.

```
#execute traceoute docs.forticare.com
traceroute to docs.forticare.com (65.39.139.196), 30 hops max, 38 byte packets
 1 172.20.120.2 (172.20.120.2) 0.324 ms 0.427 ms 0.360 ms
 2 * * *
```

If your FortiGate unit is not connected to a working DNS server, you will not be able to connect to remote host-named locations with traceroute.

tracert6

Test the connection between the FortiGate unit and another network device using IPv6 protocol, and display information about the network hops between the device and the FortiGate unit.

Syntax

```
tracert6 [-Fdn] [-f first_ttl] [-i interface] [-m max_ttl]
[-s src_addr] [-q nprobes] [-w waittime] [-z sendwait]
host [paddatalen]
```

Variable	Description
-F	Set Don't Fragment bit.
-d	Enable debugging.
-n	Do not resolve numeric address to domain name.

Variable	Description
-f <first_ttl>	Set the initial time-to-live used in the first outgoing probe packet.
-i <interface>	Select interface to use for tracer.
-m <max_ttl>	Set the max time-to-live (max number of hops) used in outgoing probe packets.
-s <src_addr>	Set the source IP address to use in outgoing probe packets.
-q <nprobes>	Set the number probes per hop.
-w <waittime>	Set the time in seconds to wait for response to a probe. Default is 5.
-z <sendwait>	Set the time in milliseconds to pause between probes.
host	Enter the IP address or FQDN to probe.
<paddatalen>	Set the packet size to use when probing.

update-av

Use this command to manually initiate the virus definitions and engines update. To update both virus and attack definitions, use the `execute update-now` command.

Syntax

```
execute update-av
```

update-geo-ip

Use this command to obtain an update to the IP geography database from FortiGuard.

Syntax

```
execute update-geo-ip
```

update-ips

Use this command to manually initiate the Intrusion Prevention System (IPS) attack definitions and engine update. To update both virus and attack definitions, use the `execute update-now` command.

Syntax

```
execute update-ips
```

update-list

Use this command to download an updated FortiGuard server list.

Syntax

```
execute update-list
```

update-now

Use this command to manually initiate both virus and attack definitions and engine updates. To initiate only virus or attack definitions, use the `execute update-av` or `execute update-ids` command respectively.

Syntax

```
execute update-now
```

update-src-vis

Use this command to trigger an FDS update of the source visibility signature package.

Syntax

```
execute update-src-vis
```

upd-vd-license

Use this command to enter a Virtual Domain (VDOM) license key.

If you have a FortiGate- unit that supports VDOM licenses, you can purchase a license key from Fortinet to increase the maximum number of VDOMs to 25, 50, 100 or 500. By default, FortiGate units support a maximum of 10 VDOMs.

Available on FortiGate models that can be licensed for more than 10 VDOMs.

Syntax

```
execute upd-vd-license <license_key>
```

Variable	Description
<license_key>	The license key is a 32-character string supplied by Fortinet. Fortinet requires your unit serial number to generate the license key.

upload

Use this command to upload system configurations and firmware images to the flash disk from FTP, TFTP, or USB sources.

Syntax

To upload configuration files:

```
execute upload config ftp <filename_str> <comment> <server_ipv4[:port_int] | server_
fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute upload config tftp <filename_str> <comment> <server_ipv4>
execute upload config usb <filename_str> <comment>
```

To upload firmware image files:

```
execute upload image ftp <filename_str> <comment> <server_ipv4[:port_int] | server_fqdn
[:port_int]> [<username_str> [<password_str>]]
execute upload image tftp <filename_str> <comment> <server_ipv4>
execute upload image usb <filename_str> <comment>
```

To upload report image files:

```
execute upload report-img ftp <filename_str> <server_ipv4[:port_int] | server_fqdn
[:port_int]> [<username_str> [<password_str>]]
execute upload report-img tftp <filename_str> <server_ipv4>
```

Variable	Description
<comment>	Comment string.
<filename_str>	Filename to upload.
<server_fqdn[:port_int]>	Server fully qualified domain name and optional port.
<server_ipv4[:port_int]>	Server IP address and optional port number.
<username_str>	Username required on server.
<password_str>	Password required on server.
<backup_password_str>	Password for backup file.

usb-device

Use these commands to manage FortiExplorer IOS devices.

Syntax

List connected FortiExplorer IOS devices

```
execute usb-device list
```

Disconnect FortiExplorer IOS devices

```
execute usb-device disconnect
```

usb-disk

Use these commands to manage your USB disks.

Syntax

```
execute usb-disk delete <filename>
execute usb-disk format
execute usb-disk list
execute usb-disk rename <old_name> <new_name>
```

Variable	Description
delete <filename>	Delete the named file from the USB disk.
format	Format the USB disk.
list	List the files on the USB disk.
rename <old_name> <new_name>	Rename a file on the USB disk.

vpn certificate ca

Use this command to import a CA certificate from a TFTP or SCEP server to the FortiGate unit, or to export a CA certificate from the FortiGate unit to a TFTP server.

Before using this command you must obtain a CA certificate issued by a CA.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate ca export tftp <certificate-name_str> <file-name_str> <tftp_ip>
execute vpn certificate ca import auto <ca_server_url> <ca_identifier_str>
execute vpn certificate ca import tftp <file-name_str> <tftp_ip>
```

Variable	Description
import	Import the CA certificate from a TFTP server to the FortiGate unit.
export	Export or copy the CA certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the CA certificate.
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.
auto	Retrieve a CA certificate from a SCEP server.
tftp	Import the CA certificate to the FortiGate unit from a file on a TFTP server (local administrator PC).
<ca_server_url>	Enter the URL of the CA certificate server.
<ca_identifier_str>	CA identifier on CA certificate server (optional).

Examples

Use the following command to import the CA certificate named `trust_ca` to the FortiGate unit from a TFTP server with the address `192.168.21.54`.

```
execute vpn certificate ca import trust_ca 192.168.21.54
```

vpn certificate crl

Use this command to get a CRL via LDAP, HTTP, or SCEP protocol, depending on the auto-update configuration.

In order to use the command `execute vpn certificate crl`, the authentication servers must already be configured.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate crl import auto <crl-name>
```

Variable	Description
import	Import the CRL from the configured LDAP, HTTP, or SCEP authentication server to the FortiGate unit.
<crl-name>	Enter the name of the CRL.
auto	Trigger an auto-update of the CRL from the configured LDAP, HTTP, or SCEP authentication server.

vpn certificate local export

Use this command to export a local certificate from the FortiGate unit to a TFTP server.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate local export tftp <certificate-name_str> <file-name_str> <tftp_ip>
```

Variable	Description
export	Export or copy the local certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the local certificate. To view a list of the local certificates, you can enter: execute vpn certificate local export tftp ?
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.

Example

Use the following command to export the local certificate request generated in the above example from the FortiGate unit to a TFTP server. The example uses the file name `testcert` for the downloaded file and the

TFTP server address 192.168.21.54.

```
execute vpn certificate local export branch_cert testcert 192.168.21.54
```

vpn certificate local generate

Use this command to generate a local certificate.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

When you generate a certificate request, you create a private and public key pair for the local FortiGate unit. The public key accompanies the certificate request. The private key remains confidential.

When you receive the signed certificate from the CA, use the `vpn certificate local` command to install it on the FortiGate unit.

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

To generate the default CA certificate used by SSL Inspection

```
execute vpn certificate local generate default-ssl-ca
```

To generate the default server key used by SSL Inspection

```
execute vpn certificate local generate default-ssl-serv-key
```

To generate an elliptical curve certificate request

```
execute vpn certificate local generate ec <certificate-name_str> <elliptic-curve-name>
<subject_str> [<optional_information>]
```

To generate an RSA certificate request

```
execute vpn certificate local generate rsa <certificate-name_str> <key-length>
<subject_str> [<optional_information>]
```

Variable	Description
<certificate-name_str>	Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

Variable	Description
<elliptic-curve-name>	Enter the elliptic curve name: <code>secp256r1</code> , <code>secp384r1</code> , or <code>secp521r1</code> .
<key-length>	Enter 1024, 1536 or 2048 for the size in bits of the encryption key.
<subject_str>	Enter the FortiGate unit host IP address, its fully qualified domain name, or an email address to identify the FortiGate unit being certified. An IP address or domain name is preferred. If this is impossible (such as with a dialup client), use an e-mail address. If you specify a host IP or domain name, use the IP address or domain name associated with the interface on which IKE negotiations will take place (usually the external interface of the local FortiGate unit). If the IP address in the certificate does not match the IP address of this interface (or if the domain name in the certificate does not match a DNS query of the FortiGate unit's IP), then some implementations of IKE may reject the connection. Enforcement of this rule varies for different IPSec products.
[<optional_information>]	Enter <code>optional_information</code> as required to further identify the certificate. See Optional information variables on page 1106 for the list of optional information variables. You must enter the optional variables in order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list. For example, to enter the <code>organization_name_str</code> , you must first enter the <code>country_code_str</code> , <code>state_name_str</code> , and <code>city_name_str</code> . While entering optional variables, you can type <code>?</code> for help on the next required variable.

Optional information variables

Variable	Description
<country_code_str>	Enter the two-character country code. Enter <code>execute vpn certificates local generate <name_str> country</code> followed by a <code>?</code> for a list of country codes. The country code is case sensitive. Enter <code>null</code> if you do not want to specify a country.
<state_name_str>	Enter the name of the state or province where the FortiGate unit is located.

Variable	Description
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiGate unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiGate unit.
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit.
<email_address_str>	Enter a contact e-mail address for the FortiGate unit.
<ca_server_url>	Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request.
<challenge_password>	Enter the challenge password for the SCEP certificate server.

Example

Use the following command to generate a local certificate request with the name `branch_cert`, the domain name `www.example.com` and a key size of 1536.

```
execute vpn certificate local generate branch_cert 1536 www.example.com
```

vpn certificate local import

Use this command to import a local certificate to the FortiGate unit from a TFTP server.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate local import tftp <file-name_str> <tftp_ip>
```

Variable	Description
<certificate-name_str>	Enter the name of the local certificate.

Variable	Description
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.

Example

Use the following command to import the signed local certificate named `branch_cert` to the FortiGate unit from a TFTP server with the address 192.168.21.54.

```
execute vpn certificate local import branch_cert 192.168.21.54
```

vpn certificate remote

Use this command to import a remote certificate from a TFTP server, or export a remote certificate from the FortiGate unit to a TFTP server. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
execute vpn certificate remote import tftp <file-name_str> <tftp_ip>
execute vpn certificate remote export tftp <certificate-name_str> <file-name_str>
<tftp_ip>
```

Field/variable	Description
import	Import the remote certificate from the TFTP server to the FortiGate unit.
export	Export or copy the remote certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the public certificate.
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.
tftp	Import/export the remote certificate via a TFTP server.

vpn ipsec tunnel down

Use this command to shut down an IPsec VPN tunnel.

Syntax

```
execute vpn ipsec tunnel down <phase2> [<phase1> <phase2_serial>]
where:
```

<phase2> is the phase 2 name
<phase1> is the phase 1 name
<phase2_serial> is the phase 2 serial number
<phase1> is required on a dial-up tunnel.

vpn ipsec tunnel up

Use this command to activate an IPsec VPN tunnel.

Syntax

```
execute vpn ipsec tunnel up <phase2> [<phase1> <phase2_serial>]
```

where:

<phase2> is the phase 2 name
<phase1> is the phase 1 name
<phase2_serial> is the phase 2 serial number

This command cannot activate a dial-up tunnel.

vpn sslvpn del-all

Use this command to delete all SSL VPN connections in this VDOM.

Syntax

```
execute vpn sslvpn del-all
```

vpn sslvpn del-tunnel

Use this command to delete an SSL tunnel connection.

Syntax

```
execute vpn sslvpn del-tunnel <tunnel_index>  
<tunnel_index> identifies which tunnel to delete if there is more than one active tunnel.
```

vpn sslvpn del-web

Use this command to delete an active SSL VPN web connection.

Syntax

```
execute vpn sslvpn del-web <web_index>
```

<web_index> identifies which web connection to delete if there is more than one active connection.

vpn sslvpn list

Use this command to list current SSL VPN tunnel connections.

Syntax

```
execute vpn sslvpn list {web | tunnel}
```

webfilter quota-reset

Use this command to reset user quota.

Syntax

```
execute webfilter quota-reset <wf-profile> <user_ip4addr>  
execute webfilter quota-reset <wf-profile> <user_name>
```

wireless-controller delete-wtp-image

Use this command to delete all firmware images for WLAN Termination Points (WTPs), also known as physical access points.

Syntax

```
execute wireless-controller delete-wtp-image
```

wireless-controller list-wtp-image

Use this command to list all firmware images for WLAN Termination Points (WTPs), also known as WiFi physical access points.

Syntax

```
execute wireless-controller list-wtp-image
```

Example output

```
WTP Images on AC:  
ImageName ImageSize(B) ImageInfo ImageMTime  
FAP22A-IMG.wtp 3711132 FAP22A-v4.0-build212 Mon Jun 6 12:26:41 2011
```

wireless-controller reset-wtp

Use this command to reset a physical access point (WTP).

If the FortiGate unit has a more recent version of the FortiAP firmware, the FortiAP unit will download and install it. Use the command [execute wireless-controller upload-wtp-image](#) to upload FortiAP firmware to the FortiGate unit.

Syntax

```
execute wireless-controller reset-wtp {<serialNumber_str> | all}
```

where `<serialNumber_str>` is the FortiWiFi unit serial number.

Use the `all` option to reset all APs.

wireless-controller restart-acd

Use this command to restart the wireless-controller daemon.

Syntax

```
execute wireless-controller restart-acd
```

wireless-controller restart-wtpd

Use this command to restart the wireless access point daemon.

Syntax

```
execute wireless-controller restart-wtpd
```

wireless-controller upload-wtp-image

Use this command to upload a FortiWiFi firmware image to the FortiGate unit. Wireless APs controlled by this wireless controller can download the image as needed. Use the [execute wireless-controller reset-wtp](#) command to trigger FortiAP units to update their firmware.

Syntax

FTP:

```
execute wireless-controller upload-wtp-image ftp <filename_str> <server_ipv4[:port_
int]> [<username_str> <password_str>]
```

TFTP:

```
execute wireless-controller upload-wtp-image tftp <filename_str> <server_ipv4>
```

get

The get commands retrieve information about the operation and performance of your FortiGate unit.

application internet-service status

Use this command to display Internet service information.

Syntax

```
get application internet-service status [<app-id>]
```

All application IDs are listed if <app-id> is not specified.

Example output

```
FG-5KD3914800284 # get application internet-service status 1245324
id: 1245324 app-name: "Fortinet-FortiGuard"
```

application internet-service-summary

Use this command to display information about the Internet service database.

Syntax

```
get application internet-service-summary
```

Example output

```
FG-5KD3914800284 # get application internet-service-summary
Version: 00002.00679
Timestamp: 201512161002
Number of Entries: 1267
```

certificate

Display detailed information about local and CA certificates installed on the FortiGate. This is a global level command. At the VDOM level, use `get vpn certificate`.

Syntax

```
get certificate {local | ca} details [certificate_name]
```


extender modem-status

Use this command to display detailed FortiExtender modem status information.

Syntax

```
get extender modem-status <serno>
```

where <serno> is the FortiExtender serial number.

Example output

```
physical_port: Internal
manufacture: Sierra Wireless, Incorporated
product: AirCard 313U
model: AirCard 313U
revision: SWI9200X_03.05.10.02AP R4684 CARMD-EN-10527 2012/02/25 11:58:38
imsi: 310410707582825
pin_status: READY
service: N/A
signal_strength: 73
RSSI: -68 dBm
connection_status: connected
Profile 1: broadband
Profile 2: broadband
Profile 13: wap.cingular
Profile 15: broadband
NAI: w.tp
Profile: 0 Disabled
home_addr: 127.219.10.128
primary_ha: 127.218.246.40
secondary_ha: 119.75.69.176
aaa_spi: 0
ha_spi: 4
esn_imei: 012615000227604
activation_status: Activated
roaming_status: N/A
usim_status: N/A
oma_dm_version: N/A
plmn: N/A
band: B17
signal_rsrq: N/A
signal_rsrp: N/A
lte_sinr: N/A
lte_rssi: N/A
lte_rs_throughput: N/A
lte_ts_throughput: N/A
lte_physical_cellid: N/A
modem_type:
drc_cdma_evdo: N/A
current_snr: N/A
wireless_operator:
operating_mode: N/A
wireless_signal: 73
usb_wan_mac: 16:78:f7:db:01:07
```

extender sys-info

Use this command to display detailed FortiExtender system information.

Syntax

```
get extender sys-info
```

firewall dnstranslation

Use this command to display the firewall DNS translation table.

Syntax

```
get firewall dnstranslation
```

firewall iprope appctrl

Use this command to list all application control signatures added to an application control list and display a summary of the application control configuration.

Syntax

```
get firewall iprope appctrl {list | status}
```

Example output

In this example, the FortiGate unit includes one application control list that blocks the FTP application.

```
get firewall iprope appctrl list
app-list=app_list_1/2000 other-action=Pass
app-id=15896 list-id=2000 action=Block
```

```
get firewall iprope appctrl status
appctrl table 3 list 1 app 1 shaper 0
```

firewall iprope list

Use this command to list all of the FortiGate unit iprope firewall policies. Optionally include a group number in hexadecimal format to display a single policy. Policies are listed in FortiOS format.

Syntax

```
get firewall iprope list [<group_number_hex>]
```

Example output

```
get firewall iprope list 0010000c

policy flag (8000000): pol_stats
flag2 (20): ep_block shapers: / per_ip=
imflag: sockport: 1011 action: redirect index: 0
schedule() group=0010000c av=00000000 au=00000000 host=0 split=00000000
chk_client_info=0x0 app_list=0 misc=0 grp_info=0 seq=0 hash=0
npu_sensor_id=0
tunnel=
zone(1): 0 ->zone(1): 0
source(0):
dest(0):
source wildcard(0):
destination wildcard(0):
service(1):
[6:0x8:1011/(0,65535)->(80,80)]
nat(0):
mms: 0 0
```

firewall proute, proute6

Use these commands to list policy routes.

Syntax

For IPv4 policy routes:

```
get firewall proute
```

For IPv6 policy routes:

```
get firewall proute6
```

Example output

```
get firewall proute
list route policy info(vf=root):
iff=5 src=1.1.1.0/255.255.255.0 tos=0x00 tos_mask=0x00 dst=0.0.0.0/0.0.0.0 protocol=80
port=1:65535
oif=3 gwy=1.2.3.4
```

firewall service custom

Use this command to view the list of custom services. If you do not specify a <service_name> the command lists all of the pre-defined services.

Syntax

```
get firewall service custom
```

This lists the services.

To view details about all services

```
config firewall service custom
show full-configuration
```

To view details about a specific service

This example lists the configuration for the ALL_TCP service:

```
config firewall service custom
edit ALL_TCP
show full-configuration
```

Example output

This is a partial output.

```
get firewall service custom
== [ ALL ]
name: ALL
== [ ALL_TCP ]
name: ALL_TCP
== [ ALL_UDP ]
name: ALL_UDP
== [ ALL_ICMP ]
name: ALL_ICMP
== [ ALL_ICMP6 ]
name: ALL_ICMP6
== [ GRE ]
name: GRE
== [ AH ]
name: AH
== [ ESP ]
name: ESP
== [ AOL ]
name: AOL
== [ BGP ]
name: BGP
== [ DHCP ]
name: DHCP
== [ DNS ]
name: DNS
== [ FINGER ]
name: FINGER
```

firewall shaper

Use these command to retrieve information about traffic shapers.

Syntax

To get information about per-ip traffic shapers

```
get firewall shaper per-ip
```

To get information about shared traffic shapers

```
get firewall shaper traffic-shaper
```

grep

In many cases the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large `get` or `show` command output you can use the `grep` command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX `grep`, used for searching text output based on regular expressions.

Information about how to use `grep` and regular expressions is available from the Internet. For example, see <http://www.opengroup.org/onlinepubs/009695399/utilities/grep.html>.

Syntax

```
{get | show| diagnose} | grep <regular_expression>
```

Example output

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr 00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
19:tcp 1110 10.31.101.10:1862 172.20.120.122:30670 69.111.193.57:1469 -
27:tcp 3599 10.31.101.10:2061 - 10.31.101.100:22 -
38:tcp 3594 10.31.101.10:4780 172.20.120.122:49700 172.20.120.100:445 -
43:tcp 3582 10.31.101.10:4398 172.20.120.122:49574 24.200.188.171:48726 -
```

Use the following command to display all lines in HTTP replacement message commands that contain URL (upper or lower case):

```
show system replacemsg http | grep -i url
set buffer "<HTML><BODY>The page you requested has been blocked because it contains a
banned word. URL = %%PROTOCOL%%URL%%</BODY></HTML>"
config system replacemsg http "url-block"
set buffer "<HTML><BODY>The URL you requested has been blocked. URL =
%%URL%%</BODY></HTML>"
config system replacemsg http "urlfilter-err"
.
.
.
```

gui console status

Display information about the CLI console.

Syntax

```
get gui console status
```

Example

The output looks like this:

```
Preferences:
  User: admin
  Colour scheme (RGB): text=FFFFFF, background=000000
  Font: style=monospace, size=10pt
  History buffer=50 lines, external input=disabled
```

hardware cpu

Use this command to display detailed information about all of the CPUs in your FortiGate unit.

Syntax

```
get hardware cpu
```

Example output

```
get hardware npu legacy list
No npu ports are found
```

```
620_ha_1 # get hardware cpu
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 15
model name : Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
stepping : 13
cpu MHz : 1795.545
cache size : 64 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 10
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
      dts acpi mmx fxsr sse sse2 ss ht tm pbe lm pni monitor ds_cpl tm2 est
bogomips : 3578.26

processor : 1
vendor_id : GenuineIntel
cpu family : 6
model : 15
model name : Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
stepping : 13
cpu MHz : 1795.545
cache size : 64 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
```

```
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 10
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
      dts acpi mmx fxsr sse sse2 ss ht tm pbe lm pn1 monitor ds_cpl tm2 est
bogomips : 3578.26
```

hardware memory

Use this command to display information about FortiGate unit memory use including the total, used, and free memory.

Syntax

```
get hardware memory
```

Example output

```
get hardware memory
total: used: free: shared: buffers: cached: shm:
Mem: 3703943168 348913664 3355029504 0 192512 139943936 137314304
Swap: 0 0 0
MemTotal: 3617132 kB
MemFree: 3276396 kB
MemShared: 0 kB
Buffers: 188 kB
Cached: 136664 kB
SwapCached: 0 kB
Active: 22172 kB
Inactive: 114740 kB
HighTotal: 1703936 kB
HighFree: 1443712 kB
LowTotal: 1913196 kB
LowFree: 1832684 kB
SwapTotal: 0 kB
SwapFree: 0 kB
```

hardware nic

Use this command to display hardware and status information about each FortiGate interface. The hardware information includes details such as the driver name and version and chip revision. Status information includes transmitted and received packets, and different types of errors.

Syntax

```
get hardware nic <interface_name>
```

Variable	Description
<interface_name>	A FortiGate interface name such as port1, wan1, internal, etc.

Example output

```

get hardware nic port9
Chip_Model FA2/ISCP1B-v3/256MB
FPGA_REV_TAG 06101916
Driver Name iscpla/b-DE
Driver Version 0.1
Driver Copyright Fortinet Inc.

Link down
Speed N/A
Duplex N/A
State up

Rx_Packets 0
Tx_Packets 0
Rx_Bytes 0
Tx_Bytes 0

Current_HWaddr 00:09:0f:77:09:68
Permanent_HWaddr 00:09:0f:77:09:68

Frame_Received 0
Bad Frame Received 0
Tx Frame 0
Tx Frame Drop 0
Receive IP Error 0
FIFO Error 0

Small PktBuf Left 125
Normal PktBuf Left 1021
Jumbo PktBuf Left 253
NAT Anomaly 0

```

hardware npu

Use this command to display information about the network processor unit (NPU) hardware installed in a FortiGate unit. The NPUs can be built-in or on an installed AMC module.

Syntax

```

get hardware npu legacy {list | session <device_name_str> | setting <device_name_str>}
get hardware npu np1 {list | status}
get hardware npu np2 {list | performance <device_id_int> | status <device_id_int>}
get hardware npu np4 {list | status <device_id_int>}
get hardware npu np6 {dce | ipsec-stats | port-list | session-stats <device_id_int> |
  sse-stats <device_id_int> | synproxy-stats}
get hardware npu sp {list | status}

```


Example output

```

get hardware npu np1 list
ID Interface
0 port9 port10

get hardware npu np1 status
ISCP1A 10ee:0702
RX SW Done 0 MTP 0x00000000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Total Number of Interfaces: 2
Number of Interface In-Use: 2
Interface[0] Tx done: 0
desc_size = 0x00004000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
Interface[1] Tx done: 0
desc_size = 0x00004000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
NAT Information:
head = 0x00000001 tail = 00000001
ISCP1A Performance [Top]:
Nr_int : 0x00000000 INTwoInd : 0x00000000 RXwoDone : 0x00000000
PKTwoEnd : 0x00000000 PKTCSErr : 0x00000000
PKTidErr : 0x00000000 PHY0Int : 0x00000000 PHY1INT : 0x00000000
CSUMOFF : 0x00000000 BADCSUM : 0x00000000 MSGINT : 0x00000000
IPSEC : 0x00000000 IPSVLAN : 0x00000000 SESMISS : 0x00000000
TOTUP : 0x00000000 RSVD MEMU : 0x00000010
MSG Performance:
QLEN: 0x00001000(QW) HEAD: 0x00000000
Performance:
TOTMSG: 0x00000000 BADMSG: 0x00000000 TOUTMSG: 0x00000000 QUERY: 0x00000000
NULLTK: 0x00000000
NAT Performance: BYPASS (Enable) BLOCK (Disable)
IRQ : 00000001 QFTL : 00000000 DELF : 00000000 FFTL : 00000000
OVTH : 00000001 QRYF : 00000000 INSF : 00000000 INVC : 00000000
ALLO : 00000000 FREE : 00000000 ALLOF : 00000000 BPENTR: 00000000 BKENTR: 00000000
PBENTR: 00000000 PBKENTR: 00000000 NOOP : 00000000 THROT : 00000000(0x002625a0)
SWITOT : 00000000 SWDTOT : 00000000 ITDB : 00000000 OTDB : 00000000
SPISES : 00000000 FLUSH : 00000000
APS (Disabled) information:
MODE: BOTH UDPTH 255 ICMPTH 255 APSFLAGS: 0x00000000
IPSEC Offload Status: 0x58077dcb

get hardware npu np2 list
ID PORTS
-- -----
0 amc-sw1/1
0 amc-sw1/2
0 amc-sw1/3
0 amc-sw1/4
ID PORTS

```

```

-- -----
1 amc-dw2/1
ID PORTS
-- -----
2 amc-dw2/2

get hardware npu np2 status 0
NP2 Status

ISCP2 f7750000 (Neighbor 00000000) 1a29:0703 256MB Base f8aad000 DBG 0x00000000
RX SW Done 0 MTP 0x0
desc_alloc = f7216000
desc_size = 0x2000 count = 0x100
nxt_to_u = 0x0 nxt_to_f = 0x0
Total Interfaces: 4 Total Ports: 4
Number of Interface In-Use: 4
Interface f7750100 netdev 81b1e000 0 Name amc-sw1-1
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750694, 00000000, 00000000, 00000000
Port f7750694 Id 0 Status Down ictr 4
desc = 8128c000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f7750100
Interface f7750264 netdev 81b2cc00 1 Name amc-sw1-2
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750748, 00000000, 00000000, 00000000
Port f7750748 Id 1 Status Down ictr 0
desc = 81287000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f7750264
Interface f77503c8 netdev 81b2c800 2 Name amc-sw1-3
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77507fc, 00000000, 00000000, 00000000
Port f77507fc Id 2 Status Down ictr 0
desc = 81286000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f77503c8
Interface f775052c netdev 81b2c400 3 Name amc-sw1-4
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77508b0, 00000000, 00000000, 00000000
Port f77508b0 Id 3 Status Down ictr 0
desc = 81281000
desc_size = 0x00001000 count = 0x00000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f775052c
NAT Information:
cmdq_qw = 0x2000 cmdq = 82160000
head = 0x1 tail = 0x1
APS (Enabled) information:
Session Install when TMM TSE OOE: Disable
Session Install when TMM TAE OOE: Disable
IPS anomaly check policy: Follow config
MSG Base = 82150000 QL = 0x1000 H = 0x0

```

hardware status

Report information about the FortiGate unit hardware including FortiASIC version, CPU type, amount of memory, flash drive size, hard disk size (if present), USB flash size (if present), network card chipset, and WiFi chipset (FortiWiFi models). This information can be useful for troubleshooting, providing information about your FortiGate unit to Fortinet Support, or confirming the features that your FortiGate model supports.

Syntax

```
get hardware status
```

Example output

```
Model name: Fortigate-620B
ASIC version: CP6
ASIC SRAM: 64M
CPU: Intel(R) Core(TM)2 Duo CPU E4300 @ 1.80GHz
RAM: 2020 MB
Compact Flash: 493 MB /dev/sda
Hard disk: 76618 MB /dev/sdb
USB Flash: not available
Network Card chipset: Broadcom 570x Tigon3 Ethernet Adapter (rev.0x5784100)
```

ips decoder status

Displays all the port settings of all the IPS decoders.

Syntax

```
get ips decoder status
```

Example output

```
# get ips decoder status
decoder-name: "back_orifice"

decoder-name: "dns_decoder"
port_list: 53

decoder-name: "ftp_decoder"
port_list: 21

decoder-name: "http_decoder"

decoder-name: "im_decoder"

decoder-name: "imap_decoder"
port_list: 143
```

Ports are shown only for decoders with configurable port settings.

ips rule status

Displays current configuration information about IPS rules.

Syntax

```
get ips rule status
```

Example output

```
# get ips rule status
rule-name: "IP.Land"
rule-id: 12588
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 3.high
service: All
location: server, client
os: All
application: All

rule-name: "IP.Loose.Src.Record.Route.Option"
rule-id: 12805
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 2.medium
service: All
location: server, client
os: All
application: All
```

ips session

Displays current IPS session status.

Syntax

```
get ips session
```

Example output

```
get ips session

SYSTEM:
memory capacity 279969792
memory used 5861008
```

```

recent pps\bps 0\0K
session in-use 0
TCP: in-use\active\total 0\0\0
UDP: in-use\active\total 0\0\0
ICMP: in-use\active\total 0\0\0

```

ips view-map

Use this command to view the policies examined by IPS. This is mainly used for debugging. If there is no ips view map, it means IPS is not used or enabled.

Syntax

```
get ips view-map <id>
```

Example output

```

id : 1
id-policy-id : 0
policy-id : 2
vdom-id : 0
which : firewall

```

Variable	Description
id	IPS policy ID
id-policy-id	Identity-based policy ID (0 means none)
policy-id	Policy ID
vdom-id	VDOM, identified by ID number
which	Type of policy id: firewall, firewall6, sniffer, sniffer6, interface, interface6

ipsec tunnel

List the current IPsec VPN tunnels and their status.

Syntax

To view details of all IPsec tunnels:

```
get ipsec tunnel details
```

To list IPsec tunnels by name:

```
get ipsec tunnel name
```

To view a summary of IPsec tunnel information:

```
get ipsec tunnel summary
```

mgmt-data status

Use this command to display information additional to that provided by `get system status` or `get hardware status`.

Syntax

```
get mgmt-data status
```

Sample output

```
FG100D3G12801361 # get mgmt-data status

Model name: FortiGate-100D
CPU: 4
RAM: 1977 MB
is_ssd_available: 0
is_logdisk_mounted: 1
is_support_log_on_boot_device: 1
is_rev_support_wanopt: 1
```

pbx branch-office

Use this command to list the configured branch offices.

Syntax

```
get pbx branch-office
```

Example output

```
== [ Branch 15 ]
name: Branch 15
== [ Branch 12 ]
name: Branch 12
```

pbx dialplan

Use this command to list the configured dial plans.

Syntax

```
get pbx dialplan
```

Example output

```
== [ company-default ]
name: company-default
== [ inbound ]
name: inbound
```

pbx did

Use this command to list the configured direct inward dial (DID) numbers.

Syntax

```
get pbx did
```

Example output

```
== [ Operator ]
name: Operator
== [ Emergency ]
name: Emergency
```

pbx extension

Use this command to list the configured extensions.

Syntax

```
get pbx extension
```

Example output

```
== [ 6555 ]
extension: 6555
== [ 6777 ]
extension: 6777
== [ 6111 ]
extension: 6111
```

pbx ftgd-voice-pkg

Use this command to display the current FortiGate Voice service package status.

Syntax

```
get pbx ftgd-voice-pkg status
```

Example output

```
Status: Activated
Total 1 Packages:
```

```
Package Type: B, Credit Left: 50.00, Credit Used: 0.00,  
Expiration Date: 2011-01-01 12:00:00
```

```
Total 1 Dids:  
12345678901  
Total 1 Efaxes:  
12345678902  
Total 0 Tollfrees:
```

pbx global

Use this command to display the current global pbx settings.

Syntax

```
get pbx global
```

Example output

```
block-blacklist : enable  
country-area : USA  
country-code : 1  
efax-check-interval : 5  
extension-pattern : 6XXX  
fax-admin-email : faxad@example.com  
ftgd-voice-server : service.fortivoice.com  
local-area-code : 408  
max-voicemail : 60  
outgoing-prefix : 9  
ring-timeout : 20  
rtp-hold-timeout : 0  
rtp-timeout : 60  
voicemail-extension : *97
```

pbx ringgrp

Use this command to display the currently configured ring groups.

Syntax

```
get pbx ringgrp
```

Example output

```
== [ 6001 ]  
name: 6001  
== [ 6002 ]  
name: 6002
```


pbx sip-trunk

Use this command to display the currently configured SIP trunks.

Syntax

```
get pbx sip-trunk
```

Example output

```
== [ __FtgdVoice_1 ]  
name: __FtgdVoice_1
```

pbx voice-menu

Use this command to display the current voice menu and recorder extension configuration.

Syntax

```
get pbx voice-menu
```

Example output

```
comment : general  
password : *  
press-0:  
ring-group : 6001  
type : ring-group  
press-1:  
type : voicemail  
press-2:  
type : directory  
press-3:  
type : none  
press-4:  
type : none  
press-5:  
type : none  
press-6:  
type : none  
press-7:  
type : none  
press-8:  
type : none  
press-9:  
type : none  
recorder-exten : *30
```

router info bfd neighbor

Use this command to list state information about the neighbors in the bi-directional forwarding table.

Syntax

```
get router info bfd neighbour
```

router info bgp

Use this command to display information about the BGP configuration.

Syntax

```
get router info bgp <keyword>
```

<keyword>	Description
cidr-only	Show all BGP routes having non-natural network masks.
community	Show all BGP routes having their COMMUNITY attribute set.
community-info	Show general information about the configured BGP communities, including the routes in each community and their associated network addresses.
community-list	Show all routes belonging to configured BGP community lists.
dampening	Display information about dampening:
{dampened-paths	Type <code>dampened-paths</code> to show all paths that have been suppressed due to flapping.
flap-statistics	Type <code>flap-statistics</code> to show flap statistics related to BGP routes.
parameters}	Type <code>parameters</code> to show the current dampening settings.
filter-list	Show all routes matching configured AS-path lists.
inconsistent-as	Show all routes associated with inconsistent autonomous systems of origin.
memory	Show the BGP memory table.

<keyword>	Description
neighbors [<address_ipv4> <address_ipv4> advertised-routes <address_ipv4> received prefix-filter <address_ipv4> received-routes <address_ipv4> routes]	Show information about connections to TCP and BGP neighbors.
network [<address_ipv4mask>]	Show general information about the configured BGP networks, including their network addresses and associated prefixes.
network-longer-prefixes <address_ipv4mask>	Show general information about the BGP route that you specify (for example, 12.0.0.0/14) and any specific routes associated with the prefix.
paths	Show general information about BGP AS paths, including their associated network addresses.
prefix-list <name>	Show all routes matching configured prefix list <name>.
quote-regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$) and enable the use of output modifiers (for example, include, exclude, and begin) to search the results.
regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$).
route-map	Show all routes matching configured route maps.
scan	Show information about next-hop route scanning, including the scan interval setting.
summary	Show information about BGP neighbor status.

Example output

```

get router info bgp memory
Memory type Alloc count Alloc bytes
=====
BGP structure : 2 1408
BGP VR structure : 2 104
BGP global structure : 1 56
BGP peer : 2 3440
BGP as list master : 1 24
Community list handler : 1 32
BGP Damp Reuse List Array : 2 4096
BGP table : 62 248
-----

```

```
Temporary memory : 4223 96095
Hash : 7 140
Hash index : 7 28672
Hash bucket : 11 132
Thread master : 1 564
Thread : 4 144
Link list : 32 636
Link list node : 24 288
Show : 1 396
Show page : 1 4108
Show server : 1 36
Prefix IPv4 : 10 80
Route table : 4 32
Route node : 63 2772
Vector : 2180 26160
Vector index : 2180 18284
Host config : 1 2
Message of The Day : 1 100
IMI Client : 1 708
VTY master : 1 20
VTY if : 11 2640
VTY connected : 5 140
Message handler : 2 120
NSM Client Handler : 1 12428
NSM Client : 1 1268
Host : 1 64
Log information : 2 72
Context : 1 232
-----
bgp proto specific allocations : 9408 B
bgp generic allocations : 196333 B
bgp total allocations : 205741 B
```

router info isis

Use this command to display information about the FortiGate ISIS.

Syntax

```
get router info isis interface
get router info isis neighbor
get router info isis is-neighbor
get router info isis database
get router info isis route
get router info isis topology
```

router info kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

Syntax

```
get router info kernel [<routing_type_int>]
```

router info multicast

Use this command to display information about a Protocol Independent Multicasting (PIM) configuration. Multicast routing is supported in the root virtual domain only.

Syntax

```
get router info multicast <keywords>
```

<keywords>	Description
igmp	<p>Show Internet Group Management Protocol (IGMP) membership information according to one of these qualifiers:</p> <p>Type <code>groups</code> [<code>{<interface-name> <group-address>}</code>] to show IGMP information for the multicast group(s) associated with the specified interface or multicast group address.</p> <p>Type <code>groups-detail</code> [<code>{<interface-name> <group-address>}</code>] to show detailed IGMP information for the multicast group(s) associated with the specified interface or multicast group address.</p> <p>Type <code>interface</code> [<code><interface-name></code>] to show IGMP information for all multicast groups associated with the specified interface.</p> <p>Show information related to dense mode operation according to one of these qualifiers:</p> <p>Type <code>interface</code> to show information about PIM-enabled interfaces.</p> <p>Type <code>interface-detail</code> to show detailed information about PIM-enabled interfaces.</p>
pim dense-mode	<p>Type <code>neighbor</code> to show the current status of PIM neighbors.</p> <p>Type <code>neighbor-detail</code> to show detailed information about PIM neighbors.</p> <p>Type <code>next-hop</code> to show information about next-hop PIM routers.</p> <p>Type <code>table</code> [<code><group-address></code>] [<code><source-address></code>] to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.</p>

<keywords>	Description
pim sparse-mode	<p>Show information related to sparse mode operation according to one of these qualifiers:</p> <p>Type <code>bsr-info</code> to show Boot Strap Router (BSR) information.</p> <p>Type <code>interface</code> to show information about PIM-enabled interfaces.</p> <p>Type <code>interface-detail</code> to show detailed information about PIM-enabled interfaces.</p> <p>Type <code>neighbor</code> to show the current status of PIM neighbors.</p> <p>Type <code>neighbor-detail</code> to show detailed information about PIM neighbors.</p> <p>Type <code>next-hop</code> to show information about next-hop PIM routers.</p> <p>Type <code>rp-mapping</code> to show Rendezvous Point (RP) information.</p> <p>Type <code>table [<group-address> [<source-address>]</code> to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.</p>
table [<group-address>] [<source-address>]	<p>Show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.</p>
table-count [<group-address>] [<source-address>]	<p>Show statistics related to the specified multicast group address and/or multicast source address.</p>

router info ospf

Use this command to display information about the FortiGate OSPF configuration and/or the Link-State Advertisements (LSAs) that the FortiGate unit obtains and generates. An LSA identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination.

Syntax

```
get router info ospf <keyword>
```

<keyword>	Description
border-routers	<p>Show OSPF routing table entries that have an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) as a destination.</p>

<keyword>	Description
database <qualifier>	<p>Show information from the OSPF routing database according to the of these qualifiers.</p> <p>Some qualifiers require a <code>target</code> that can be one of the following values:</p> <p>Type <code>adv_router <address_ipv4></code> to limit the information to LSAs originating from the router at the specified IP address.</p> <p>Type <code>self-originate <address_ipv4></code> to limit the information to LSAs originating from the FortiGate unit.</p>
adv-router <address_ipv4>	Type <code>adv-router <address_ipv4></code> to show ospf Advertising Router link states for the router at the given IP address.
asbr-summary <target>	Type <code>asbr-summary</code> to show information about ASBR summary LSAs.
brief	Type <code>brief</code> to show the number and type of LSAs associated with each OSPF area.
external <target>	Type <code>external</code> to show information about external LSAs.
max-age	Type <code>max-age</code> to show all LSAs in the MaxAge list.
network <target>	Type <code>network</code> to show information about network LSAs.
nssa-external <target>	Type <code>nssa-external</code> to show information about not-so-stubby external LSAs.
opaque-area <address_ipv4>	Type <code>opaque-area <address_ipv4></code> to show information about opaque Type 10 (area-local) LSAs (see RFC 2370).
opaque-as <address_ipv4>	Type <code>opaque-as <address_ipv4></code> to show information about opaque Type 11 LSAs (see RFC 2370), which are flooded throughout the AS.
opaque-link <address_ipv4>	Type <code>opaque-link <address_ipv4></code> to show information about opaque Type 9 (link-local) LSAs (see RFC 2370).

<keyword>	Description
router <target>	Type <code>router</code> to show information about router LSAs.
self-originate	Type <code>self-originate</code> to show self-originated LSAs.
summary <target>	Type <code>summary</code> to show information about summary LSAs.
interface [<interface_name>]	Show the status of one or all FortiGate interfaces and whether OSPF is enabled on those interfaces.
	Show general information about OSPF neighbors, excluding down-status neighbors:
	Type <code>all</code> to show information about all neighbors, including down-status neighbors.
	Type <code><neighbor_id></code> to show detailed information about the specified neighbor only.
neighbor [all <neighbor_id> detail detail all interface <address_ipv4>]	Type <code>detail</code> to show detailed information about all neighbors, excluding down-status neighbors.
	Type <code>detail all</code> to show detailed information about all neighbors, including down-status neighbors.
	Type <code>interface <address_ipv4></code> to show neighbor information based on the FortiGate interface IP address that was used to establish the neighbor's relationship.
route	Show the OSPF routing table.
status	Show general information about the OSPF routing processes.
virtual-links	Show information about OSPF virtual links.

router info protocols

Use this command to show the current states of active routing protocols. Inactive protocols are not displayed.

Syntax

```
get router info protocols
```

```
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
```



```

Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
Routing for Networks:
Routing Information Sources:
Gateway Distance Last Update Bad Packets Bad Routes
Distance: (default is 120)

Routing Protocol is "ospf 0"
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing:
Routing for Networks:
Routing Information Sources: Gateway Distance Last Update
Distance: (default is 110) Address Mask Distance List

Routing Protocol is "bgp 5"
IGP synchronization is disabled
Automatic route summarization is disabled
Default local-preference applied to incoming route is 100
Redistributing:
Neighbor(s):
Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn RouteMapOut Weight
192.168.20.10 unicast

```

router info rip

Use this command to display information about the RIP configuration.

Syntax

```
get router info rip <keyword>
```

<keyword>	Description
database	Show the entries in the RIP routing database.
interface	Show the status of the specified FortiGate unit interface <interface_name> and whether RIP is enabled.
[<interface_name>]	If interface is used alone it lists all the FortiGate unit interfaces and whether RIP is enabled on each.

router info routing-table

Use this command to display the routes in the routing table.

Syntax

```
get router info routing-table <keyword>
```

<keyword>	Description
all	Show all entries in the routing table.
bgp	Show the BGP routes in the routing table.
connected	Show the connected routes in the routing table.
database	Show the routing information database.
details [<address_ ipv4mask>]	Show detailed information about a route in the routing table, including the next-hop routers, metrics, outgoing interfaces, and protocol-specific information.
ospf	Show the OSPF routes in the routing table.
rip	Show the RIP routes in the routing table.
static	Show the static routes in the routing table.

router info vrrp

Use this command to display information about the VRRP configuration.

Syntax

```
get router info vrrp
```

Example output

```
Interface: port1, primary IP address: 9.1.1.2
VRID: 1
  vrip: 9.1.1.254, priority: 100, state: BACKUP
  adv_interval: 1, preempt: 1, start_time: 3
  vrdst: 0.0.0.0
```

router info6 bgp

Use this command to display information about the BGP IPv6 configuration.

Syntax

```
get router info6 bgp <keyword>
```

<keyword>	Description
community	Show all BGP routes having their COMMUNITY attribute set.

<keyword>	Description
community-list	Show all routes belonging to configured BGP community lists.
	Display information about dampening:
dampening {dampened-paths flap-statistics parameters}	Type <code>dampened-paths</code> to show all paths that have been suppressed due to flapping.
	Type <code>flap-statistics</code> to show flap statistics related to BGP routes.
	Type <code>parameters</code> to show the current dampening settings.
filter-list	Show all routes matching configured AS-path lists.
inconsistent-as	Show all routes associated with inconsistent autonomous systems of origin.
neighbors [<address_ ipv6mask>	Show information about connections to TCP and BGP neighbors.
network [<address_ ipv6mask>]	Show general information about the configured BGP networks, including their network addresses and associated prefixes.
network-longer- prefixes <address_ ipv6mask>	Show general information about the BGP route that you specify (for example, <code>12.0.0.0/14</code>) and any specific routes associated with the prefix.
paths	Show general information about BGP AS paths, including their associated network addresses.
prefix-list <name>	Show all routes matching configured prefix list <name>.
quote-regexp <regexp_str>	Enter the regular expression to compare to the <code>AS_PATH</code> attribute of BGP routes (for example, <code>^730\$</code>) and enable the use of output modifiers (for example, <code>include</code> , <code>exclude</code> , and <code>begin</code>) to search the results.
regexp <regexp_str>	Enter the regular expression to compare to the <code>AS_PATH</code> attribute of BGP routes (for example, <code>^730\$</code>).
route-map	Show all routes matching configured route maps.
summary	Show information about BGP neighbor status.

router info6 interface

Use this command to display information about IPv6 interfaces.

Syntax

```
get router info6 interface <interface_name>
```

Example output

The command returns the status of the interface and the assigned IPv6 address.

```
dmz2 [administratively down/down]  
2001:db8:85a3:8d3:1319:8a2e:370:7348  
fe80::209:fff:fe04:4cfd
```

router info6 kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

Syntax

```
get router info6 kernel
```

router info6 ospf

Use this command to display information about the OSPF IPv6 configuration.

Syntax

```
get router info6 ospf
```

router info6 protocols

Use this command to display information about the configuration of all IPv6 dynamic routing protocols.

Syntax

```
get router info6 protocols
```

router info6 rip

Use this command to display information about the RIPng configuration.

Syntax

```
get router info6 rip
```

router info6 routing-table

Use this command to display the routes in the IPv6 routing table.

Syntax

```
get router info6 routing-table <item>
```

where <item> is one of the following:

Variable	Description
<ipv6_ip>	Destination IPv6 address or prefix.
bgp	Show BGP routing table entries.
connected	Show connected routing table entries.
database	Show routing information base.
ospf	Show OSPF routing table entries.
rip	Show RIP routing table entries.
static	Show static routing table entries.

switch-controller poe

Retrieve information about PoE ports.

Syntax

```
get switch-controller poe <vdom-name> <fortiswitch-id>
```

system admin list

View a list of all the current administration sessions.

Syntax

```
get system admin list
```

Example output

```
# get system admin list
username local  device                remote                started
admin    sshv2  port1:172.20.120.148:22  172.20.120.16:4167  2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443  172.20.120.161:56365  2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443  172.20.120.16:4214  2006-08-09 12:25:29
```

Variable	Description
username	Name of the admin account for this session
local	The protocol this session used to connect to the FortiGate unit.
device	The interface, IP address, and port used by this session to connect to the FortiGate unit.
remote	The IP address and port used by the originating computer to connect to the FortiGate unit.
started	The time the current session started.

system admin status

View the status of the currently logged in admin and their session.

Syntax

```
get system admin status
```

Example

The output looks like this:

```
# get system admin status
username: admin
login local: sshv2
login device: port1:172.20.120.148:22
login remote: 172.20.120.16:4167
login vdom: root
login started: 2006-08-09 12:24:20
current time: 2006-08-09 12:32:12
```

Variable	Description
username	Name of the admin account currently logged in.
login local	The protocol used to start the current session.
login device	The login information from the FortiGate unit including interface, IP address, and port number.
login remote	The computer the user is logging in from including the IP address and port number.
login vdom	The virtual domain the admin is current logged into.
login started	The time the current session started.
current time	The current time of day on the FortiGate unit

system arp

View the ARP table entries on the FortiGate unit.

This command is not available in multiple VDOM mode.

Syntax

```
get system arp
```

Example output

```
# get system arp
Address Age(min) Hardware Addr Interface
172.20.120.16 0 00:0d:87:5c:ab:65 internal
172.20.120.138 0 00:08:9b:09:bb:01 internal
```

system auto-update

Use this command to display information about the status FortiGuard updates on the FortiGate unit.

Syntax

```
get system auto-update status
get system auto-update versions
```

Example output

```
get system auto-update status
FDN availability: available at Thu Apr 1 08:22:58 2010

Push update: disable
Scheduled update: enable
    Update daily: 8:22
Virus definitions update: enable
IPS definitions update: enable
Server override: disable
Push address override: disable
Web proxy tunneling: disable
```

system central-management

View information about the Central Management System configuration.

Syntax

```
get system central-management
```

Example

The output looks like this:

```
FG600B3908600705 # get system central-management
status : enable
type : fortimanager
auto-backup : disable
schedule-config-restore: enable
schedule-script-restore: enable
allow-push-configuration: enable
allow-pushd-firmware: enable
allow-remote-firmware-upgrade: enable
allow-monitor : enable
fmg : 172.20.120.161
vdom : root
authorized-manager-only: enable
serial-number : "FMG-3K2404400063"
```

system checksum

View the checksums for global, root, and all configurations. These checksums are used by HA to compare the configurations of each cluster unit.

Syntax

```
get system checksum status
```

Example output

```
# get system checksum status
global: 7a 87 3c 14 93 bc 98 92 b0 58 16 f2 eb bf a4 15
root: bb a4 80 07 42 33 c2 ff f1 b5 6e fe e4 bb 45 fb
all: 1c 28 f1 06 fa 2e bc 1f ed bd 6b 21 f9 4b 12 88
```

system cmdb status

View information about cmdbsvr on the FortiGate unit. FortiManager uses some of this information.

Syntax

```
get system cmdb status
```

Example output

```
# get system cmdb status
version: 1
owner id: 18
update index: 6070
config checksum: 12879299049430971535
last request pid: 68
last request type: 29
last request: 78
```


Variable	Description
version	Version of the cmdb software.
owner id	Process ID of the cmdbsvr daemon.
update index	The updated index shows how many changes have been made in cmdb.
config checksum	The config file version used by FortiManager.
last request pid	The last process to access the cmdb.
last request type	Type of the last attempted access of cmdb.
last request	The number of the last attempted access of cmdb.

system fortianalyzer-connectivity

Display connection and remote disk usage information about a connected FortiAnalyzer unit.

Syntax

```
get fortianalyzer-connectivity status
```

Example output

```
# get system fortianalyzer-connectivity status
Status: connected
Disk Usage: 0%
```

system fortiguard-log-service status

Command returns information about the status of the FortiGuard Log & Analysis Service including license and disk information.

Syntax

```
get system fortiguard-log-service status
```

Example output

```
# get system fortiguard-log-service status
FortiGuard Log & Analysis Service
Expire on: 20071231
Total disk quota: 1111 MB
Max daily volume: 111 MB
Current disk quota usage: n/a
```

system fortiguard-service status

COMMAND REPLACED. Command returns information about the status of the FortiGuard service including the name, version late update, method used for the last update and when the update expires. This information is shown for the AV Engine, virus definitions, attack definitions, and the IPS attack engine.

Syntax

```
get system fortiguard-service status
```

Example output

NAME	VERSION	LAST UPDATE	METHOD	EXPIRE
AV Engine	2.002	2006-01-26 19:45:00	manual	2006-06-12 08:00:00
Virus Definitions	6.513	2006-06-02 22:01:00	manual	2006-06-12 08:00:00
Attack Definitions	2.299	2006-06-09 19:19:00	manual	2006-06-12 08:00:00
IPS Attack Engine	1.015	2006-05-09 23:29:00	manual	2006-06-12 08:00:00

system ha-nonsync-csum

FortiManager uses this command to obtain a system checksum.

Syntax

```
get system ha-nonsync-csum
```

system ha status

Use this command to display information about an HA cluster. The command displays general HA configuration settings. The command also displays information about how the cluster unit that you have logged into is operating in the cluster.

Usually you would log into the primary unit CLI using SSH or telnet. In this case the `get system ha status` command displays information about the primary unit first, and also displays the HA state of the primary unit (the primary unit operates in the work state). However, if you log into the primary unit and then use the `execute ha manage` command to log into a subordinate unit, (or if you use a console connection to log into a subordinate unit) the `get system status` command displays information about this subordinate unit first, and also displays the HA state of this subordinate unit. The state of a subordinate unit is work for an active-active cluster and standby for an active-passive cluster.

For a virtual cluster configuration, the `get system ha status` command displays information about how the cluster unit that you have logged into is operating in virtual cluster 1 and virtual cluster 2. For example, if you connect to the cluster unit that is the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2, the output of the `get system ha status` command shows virtual cluster 1 in the work state and virtual cluster 2 in the standby state. The `get system ha status` command also displays additional information about virtual cluster 1 and virtual cluster 2.

Syntax

```
get system ha status
```

The command display includes the following fields. For more information see the examples that follow.

Variable	Description
Model	The FortiGate model number.
Mode	The HA mode of the cluster: a-a or a-p.
Group	The group ID of the cluster.
Debug	The debug status of the cluster.
ses_pickup	The status of session pickup: enable or disable.
load_balance	The status of the <code>load-balance-all</code> field: enable or disable. Displayed for active-active clusters only.
schedule	The active-active load balancing schedule. Displayed for active-active clusters only.
Master	<p><code>Master</code> displays the device priority, host name, serial number, and actual cluster index of the primary (or master) unit.</p> <p><code>Slave</code> displays the device priority, host name, serial number, and actual cluster index of the subordinate (or slave, or backup) unit or units.</p>
Slave	<p>The list of cluster units changes depending on how you log into the CLI. Usually you would use SSH or telnet to log into the primary unit CLI. In this case the primary unit would be at the top the list followed by the other cluster units.</p> <p>If you use <code>execute ha manage</code> or a console connection to log into a subordinate unit CLI, and then enter <code>get system ha status</code> the subordinate unit that you have logged into appears at the top of the list of cluster units.</p>
number of vcluster	The number of virtual clusters. If virtual domains are not enabled, the cluster has one virtual cluster. If virtual domains are enabled the cluster has two virtual clusters.

Variable	Description
vcluster 1	<p>The HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 1. If virtual domains are not enabled, <code>vcluster 1</code> displays information for the cluster. If virtual domains are enabled, <code>vcluster 1</code> displays information for virtual cluster 1.</p> <p>The HA heartbeat IP address is 10.0.0.1 if you are logged into a the primary unit of virtual cluster 1 and 10.0.0.2 if you are logged into a subordinate unit of virtual cluster 1.</p> <p><code>vcluster 1</code> also lists the primary unit (master) and subordinate units (slave) in virtual cluster 1. The list includes the operating cluster index and serial number of each cluster unit in virtual cluster 1. The cluster unit that you have logged into is at the top of the list.</p> <p>If virtual domains are not enabled and you connect to the primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the primary unit.</p> <p>If virtual domains are not enabled and you connect to a subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you have logged into.</p> <p>If virtual domains are enabled and you connect to the virtual cluster 1 primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the virtual cluster 1 primary unit.</p> <p>If virtual domains are enabled and you connect to the virtual cluster 1 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you are logged into.</p> <p>In a cluster consisting of two cluster units operating without virtual domains enabled all clustering actually takes place in virtual cluster 1. HA is designed to work this way to support virtual clustering. If this cluster was operating with virtual domains enabled, adding virtual cluster 2 is similar to adding a new copy of virtual cluster 1. Virtual cluster 2 is visible in the <code>get system ha status</code> command output when you add virtual domains to virtual cluster 2.</p>

Variable	Description
vcluster 2	<p><code>vcluster 2</code> only appears if virtual domains are enabled.</p> <p><code>vcluster 2</code> displays the HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 2. The HA heartbeat IP address is 10.0.0.2 if you are logged into the primary unit of virtual cluster 2 and 10.0.0.1 if you are logged into a subordinate unit of virtual cluster 2.</p> <p><code>vcluster 2</code> also lists the primary unit (master) and subordinate units (slave) in virtual cluster 2. The list includes the cluster index and serial number of each cluster unit in virtual cluster 2. The cluster unit that you have logged into is at the top of the list.</p> <p>If you connect to the virtual cluster 2 primary unit CLI, the HA state of the cluster unit in virtual cluster 2 is <code>work</code>. The display lists the cluster units starting with the virtual cluster 2 primary unit.</p> <p>If you connect to the virtual cluster 2 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 2 is <code>standby</code>. The display lists the cluster units starting with the subordinate unit that you are logged into.</p>

system info admin status

Use this command to display administrators that are logged into the FortiGate unit.

Syntax

```
get system info admin status
```

Example

This shows sample output.

```
Index User name Login type From
0 admin CLI ssh(172.20.120.16)
1 admin WEB 172.20.120.16
```

Variable	Description
Index	The order the administrators logged in.
User name	The name of the user account logged in.
Login type	Which interface was used to log in.
From	The IP address this user logged in from.

Related topics

"system info admin ssh" on page 1150

system info admin ssh

Use this command to display information about the SSH configuration on the FortiGate unit such as:

the SSH port number

the interfaces with SSH enabled

the hostkey DSA fingerprint

the hostkey RSA fingerprint

Syntax

```
get system info admin ssh
```

Example output

```
# get system info admin ssh
SSH v2 is enabled on port 22
SSH is enabled on the following 1 interfaces:
internal
SSH hostkey DSA fingerprint = cd:e1:87:70:bb:f0:9c:7d:e3:7b:73:f7:44:23:a5:99
SSH hostkey RSA fingerprint = c9:5b:49:1d:7c:ba:be:f3:9d:39:33:4d:48:9d:b8:49
```

system interface physical

Use this command to list information about the unit's physical network interfaces.

Syntax

```
get system interface physical
```

The output looks like this:

```
# get system interface physical
== [onboard]
==[dmz1]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[dmz2]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[internal]
mode: static
ip: 172.20.120.146 255.255.255.0
status: up
```

```
speed: 100
==[wan1]
mode: pppoe
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[wan2]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
==[modem]
mode: static
ip: 0.0.0.0 0.0.0.0
status: down
speed: n/a
```

system ip-conflict status

List interface names and IP addresses in conflict.

Syntax

```
get system ip-conflict status
```

system mgmt-csum

FortiManager uses this command to obtain checksum information from FortiGate units.

Syntax

```
get system mgmt-csum {global | vdom | all}
```

where

`global` retrieves global object checksums

`vdom` retrieves VDOM object checksums

`all` retrieves all object checksums.

system performance firewall

Use this command to display packet distribution and traffic statistics information for the FortiGate firewall.

Syntax

```
get system performance firewall packet-distribution
get system performance firewall statistics
```

Variable	Description
packet-distribution	<p>Display a list of packet size ranges and the number of packets of each size accepted by the firewall since the system restarted. You can use this information to learn about the packet size distribution on your network.</p> <p>Note: these counts do not include packets offloaded to the NPU.</p>
statistics	<p>Display a list of traffic types (browsing, email, DNS etc) and the number of packets and number of payload bytes accepted by the firewall for each type since the FortiGate unit was restarted.</p>

Example output

```

get system performance firewall packet-distribution
getting packet distribution statistics...
0 bytes - 63 bytes: 655283 packets
64 bytes - 127 bytes: 1678278 packets
128 bytes - 255 bytes: 58823 packets
256 bytes - 383 bytes: 70432 packets
384 bytes - 511 bytes: 1610 packets
512 bytes - 767 bytes: 3238 packets
768 bytes - 1023 bytes: 7293 packets
1024 bytes - 1279 bytes: 18865 packets
1280 bytes - 1500 bytes: 58193 packets
> 1500 bytes: 0 packets

get system performance firewall statistics
getting traffic statistics...
Browsing: 623738 packets, 484357448 bytes
DNS: 5129187383836672 packets, 182703613804544 bytes
E-Mail: 23053606 packets, 2 bytes
FTP: 0 packets, 0 bytes
Gaming: 0 packets, 0 bytes
IM: 0 packets, 0 bytes
Newsgroups: 0 packets, 0 bytes
P2P: 0 packets, 0 bytes
Streaming: 0 packets, 0 bytes
TFTP: 654722117362778112 packets, 674223966126080 bytes
VoIP: 16834455 packets, 10 bytes
Generic TCP: 266287972352 packets, 8521215115264 bytes
Generic UDP: 0 packets, 0 bytes
Generic ICMP: 0 packets, 0 bytes
Generic IP: 0 packets, 0 bytes

```

system performance status

Use this command to display FortiGate CPU usage, memory usage, network usage, sessions, virus, IPS attacks, and system up time.

Syntax

```
get system performance status
```

Variable	Description
CPU states	<p>The percentages of CPU cycles used by user, system, nice and idle categories of processes. These categories are:</p> <p><code>user</code> -CPU usage of normal user-space processes</p> <p><code>system</code> -CPU usage of kernel</p> <p><code>nice</code> - CPU usage of user-space processes having other-than-normal running priority</p> <p><code>idle</code> - Idle CPU cycles</p> <p>Adding <code>user</code>, <code>system</code>, and <code>nice</code> produces the total CPU usage as seen on the CPU widget on the web-based system status dashboard.</p>
Memory states	The percentage of memory used.
Average network usage	The average amount of network traffic in kbps in the last 1, 10 and 30 minutes.
Average sessions	The average number of sessions connected to the FortiGate unit over the last 1, 10 and 30 minutes.
Virus caught	The number of viruses the FortiGate unit has caught in the last 1 minute.
IPS attacks blocked	The number of IPS attacks that have been blocked in the last 1 minute.
Uptime	How long since the FortiGate unit has been restarted.

Example output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
Memory states: 18% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 1 kbps in 30 minutes
Average sessions: 5 sessions in 1 minute, 6 sessions in 10 minutes, 5 sessions in 30
minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 9days, 22 hours, 0 minutes
```

system performance top

Use this command to display the list of processes running on the FortiGate unit (similar to the Linux `top` command).

You can use the following commands when `get system performance top` is running:

- Press Q or Ctrl+C to quit.
- Press P to sort the processes by the amount of CPU that the processes are using.
- Press M to sort the processes by the amount of memory that the processes are using.

Syntax

```
get system performance top [<delay_int>] <max_lines_int>]]
```

Variable	Description
<delay_int>	The delay, in seconds, between updating the process list. The default is 5 seconds.
<max_lines_int>	The maximum number of processes displayed in the output. The default is 20 lines.

system session list

Command returns a list of all the sessions active on the FortiGate unit, or the current virtual domain if virtual domain mode is enabled.

Syntax

```
get system session list
```

Example output

```

PROTO      EXPIRE  SOURCE          SOURCE-NAT  DESTINATION  DESTINATION-NAT
tcp 0 127.0.0.1:1083 -      127.0.0.1:514 -
tcp 0 127.0.0.1:1085 -      127.0.0.1:514 -
tcp 10 127.0.0.1:1087 -      127.0.0.1:514 -
tcp 20 127.0.0.1:1089 -      127.0.0.1:514 -
tcp 30 127.0.0.1:1091 -      127.0.0.1:514 -
tcp 40 127.0.0.1:1093 -      127.0.0.1:514 -
tcp 60 127.0.0.1:1097 -      127.0.0.1:514 -
tcp 70 127.0.0.1:1099 -      127.0.0.1:514 -
tcp 80 127.0.0.1:1101 -      127.0.0.1:514 -
tcp 90 127.0.0.1:1103 -      127.0.0.1:514 -
tcp 100 127.0.0.1:1105 -      127.0.0.1:514 -
tcp 110 127.0.0.1:1107 -      127.0.0.1:514 -
tcp 103 172.20.120.16:3548 -      172.20.120.133:22 -
tcp 3600 172.20.120.16:3550 -      172.20.120.133:22 -
udp 175 127.0.0.1:1026 -      127.0.0.1:53 -
tcp 5 127.0.0.1:1084 -      127.0.0.1:514 -
tcp 5 127.0.0.1:1086 -      127.0.0.1:514 -
tcp 15 127.0.0.1:1088 -      127.0.0.1:514 -
tcp 25 127.0.0.1:1090 -      127.0.0.1:514 -
tcp 45 127.0.0.1:1094 -      127.0.0.1:514 -
tcp 59 127.0.0.1:1098 -      127.0.0.1:514 -
tcp 69 127.0.0.1:1100 -      127.0.0.1:514 -
tcp 79 127.0.0.1:1102 -      127.0.0.1:514 -

```

```
tcp 99 127.0.0.1:1106 -      127.0.0.1:514 -
tcp 109 127.0.0.1:1108 -     127.0.0.1:514 -
tcp 119 127.0.0.1:1110 -     127.0.0.1:514 -
```

Variable	Description
PROTO	The transfer protocol of the session.
EXPIRE	How long before this session will terminate.
SOURCE	The source IP address and port number.
SOURCE-NAT	The source of the NAT. '-' indicates there is no NAT.
DESTINATION	The destination IP address and port number.
DESTINATION-NAT	The destination of the NAT. '-' indicates there is no NAT.

system session status

Use this command to display the number of active sessions on the FortiGate unit, or if virtual domain mode is enabled it returns the number of active sessions on the current VDOM. In both situations it will say 'the current VDOM'.

Syntax

```
get system session status
```

Example output

```
The total number of sessions for the current VDOM: 3100
```

system session-helper-info list

Use this command to list the FortiGate session helpers and the protocol and port number configured for each one.

Syntax

```
get system session-helper-info list
```

Example output

```
list builtin help module:
mgcp
dcerpc
rsh
pmap
dns-tcp
dns-udp
rtsp
pptp
```

```

sip
mms
tns
h245
h323
ras
tftp
ftp
list session help:
help=pmap, protocol=17 port=111
help=rtsp, protocol=6 port=8554
help=rtsp, protocol=6 port=554
help=pptp, protocol=6 port=1723
help=rtsp, protocol=6 port=7070
help=sip, protocol=17 port=5060
help=pmap, protocol=6 port=111
help=rsh, protocol=6 port=512
help=dns-udp, protocol=17 port=53
help=tftp, protocol=17 port=69
help=tns, protocol=6 port=1521
help=mgcp, protocol=17 port=2727
help=dcerpc, protocol=17 port=135
help=rsh, protocol=6 port=514
help=ras, protocol=17 port=1719
help=ftp, protocol=6 port=21
help=mgcp, protocol=17 port=2427
help=dcerpc, protocol=6 port=135
help=mms, protocol=6 port=1863
help=h323, protocol=6 port=1720

```

system session-info

Use this command to display session information.

Syntax

```

get system session-info expectation
get system session-info full-stat
get system session-info list
get system session-info statistics
get system session-info ttl

```

Variable	Description
expectation	Display expectation sessions.
full-stat	Display detailed information about the FortiGate session table including a session table and expect session table summary, firewall error statistics, and other information.

Variable	Description
list	Display detailed information about all current FortiGate sessions. For each session the command displays the protocol number, traffic shaping information, policy information, state information, statistics and other information.
statistics	Display the same information as the <code>full-stat</code> command except for the session table and expect session table summary.
tll	Display the current setting of the <code>config system session-ttl</code> command including the overall session timeout as well as the timeouts for specific protocols.

Example output

```
get system session-info statistics
misc info: session_count=15 exp_count=0 clash=0 memory_tension_drop=0 ephemeral=1/32752
          removeable=14
delete=0, flush=0, dev_down=0/0
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000001
tcp reset stat:
syncqf=0 acceptqf=0 no-listener=227 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

system source-ip

Use this command to list defined source-IPs.

Syntax

```
get system source-ip
```

Example output

```
# get sys source-ip status
The following services force their communication to use
a specific source IP address:

service=NTP source-ip=172.18.19.101
service=DNS source-ip=172.18.19.101
vdom=root service=RADIUS name=server-pc25 source-ip=10.1.100.101
vdom=root service=TACACS+ name=tac_plus_pc25 source-ip=10.1.100.101
```

```
vdom=root service=FSAE name=pc26 source-ip=172.18.19.101
vdom=V1 service=RADIUS name=pc25-Radius source-ip=172.16.200.101
vdom=V1 service=TACACS+ name=pc25-tacacs+ source-ip=172.16.200.101
vdom=V1 service=FSAE name=pc16 source-ip=172.16.200.101
```

system startup-error-log

Use this command to display information about system startup errors. This command only displays information if an error occurs when the FortiGate unit starts up.

Syntax

```
get system startup-error-log
```

system stp list

Use this command to display Spanning Tree Protocol status.

Syntax

```
get system stp list
```

system status

Use this command to display system status information including:

FortiGate firmware version, build number and branch point

virus and attack definitions version

FortiGate unit serial number and BIOS version

log hard disk availability

host name

operation mode

virtual domains status: current VDOM, max number of VDOMs, number of NAT and TP mode VDOMs and VDOM status

current HA status

system time

the revision of the WiFi chip in a FortiWiFi unit

Syntax

```
get system status
```

Example output

```
Version: Fortigate-620B v4.0,build0271,100330 (MR2)
Virus-DB: 11.00643(2010-03-31 17:49)
Extended DB: 11.00643(2010-03-31 17:50)
Extreme DB: 0.00000(2003-01-01 00:00)
IPS-DB: 2.00778(2010-03-31 12:55)
FortiClient application signature package: 1.167(2010-04-01 10:11)
Serial-Number: FG600B3908600705
BIOS version: 04000006
Log hard disk: Available
Hostname: 620_ha_1
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Distribution: International
Branch point: 271
Release Version Information: MR2
System time: Thu Apr 1 15:27:29 2010
```

test

Use this command to display information about FortiGate applications and perform operations on FortiGate applications. You can specify an application name and a test level. Enter ? to display the list of applications. The test level performs various functions depending on the application but can include displaying memory usage, dropping connections and restarting the application.

The test levels are different for different applications. In some cases when you enter the command and include an application name but no test level (or an invalid test level) the command output includes a list of valid test levels.

Syntax

```
get test <application_name_str> <test_level_int>
```

Example output

```
get test http
Proxy Worker 0 - http
[0:H] HTTP Proxy Test Usage
[0:H]
[0:H] 2: Drop all connections
[0:H] 22: Drop max idle connections
[0:H] 222: Drop all idle connections
[0:H] 4: Display connection stat
[0:H] 44: Display info per connection
[0:H] 444: Display connections per state
[0:H] 4444: Display per-VDOM statistics
[0:H] 44444: Display information about idle connections
[0:H] 55: Display tcp info per connection
```

```
get test http 4
HTTP Common
Current Connections 0/8032

HTTP Stat
Bytes sent 0 (kb)
Bytes received 0 (kb)
Error Count (alloc) 0
Error Count (accept) 0
Error Count (bind) 0
Error Count (connect) 0
Error Count (socket) 0
Error Count (read) 0
Error Count (write) 0
Error Count (retry) 0
Error Count (poll) 0
Error Count (scan reset) 0
Error Count (urlfilter wait) 0
Last Error 0
Web responses clean 0
Web responses scan errors 0
Web responses detected 0
Web responses infected with worms 0
Web responses infected with viruses 0
Web responses infected with susp 0
Web responses file blocked 0
Web responses file exempt 0
Web responses bannedword detected 0
Web requests oversize pass 0
Web requests oversize block 0
URL requests exempt 0
URL requests blocked 0
URL requests passed 0
URL requests submit error 0
URL requests rating error 0
URL requests rating block 0
URL requests rating allow 0
URL requests infected with worms 0
Web requests detected 0
Web requests file blocked 0
Web requests file exempt 0
POST requests clean 0
POST requests scan errors 0
POST requests infected with viruses 0
POST requests infected with susp 0
POST requests file blocked 0
POST requests bannedword detected 0
POST requests oversize pass 0
POST requests oversize block 0
Web request backlog drop 0
Web response backlog drop 0

HTTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
urlfilter=0/0/0 uf_lookupf=0
scan=0 clt=0 srv=0
```


user adgrp

Use this command to list Directory Service user groups.

Syntax

```
get user adgrp [<dsgroupname>]
```

If you do not specify a group name, the command returns information for all Directory Service groups. For example:

```
== [ DOCTEST/Cert Publishers ]
name: DOCTEST/Cert Publishers server-name: DSserv1
== [ DOCTEST/Developers ]
name: DOCTEST/Developers server-name: DSserv1
== [ DOCTEST/Domain Admins ]
name: DOCTEST/Domain Admins server-name: DSserv1
== [ DOCTEST/Domain Computers ]
name: DOCTEST/Domain Computers server-name: DSserv1
== [ DOCTEST/Domain Controllers ]
name: DOCTEST/Domain Controllers server-name: DSserv1
== [ DOCTEST/Domain Guests ]
name: DOCTEST/Domain Guests server-name: DSserv1
== [ DOCTEST/Domain Users ]
name: DOCTEST/Domain Users server-name: DSserv1
== [ DOCTEST/Enterprise Admins ]
name: DOCTEST/Enterprise Admins server-name: DSserv1
== [ DOCTEST/Group Policy Creator Owners ]
name: DOCTEST/Group Policy Creator Owners server-name: DSserv1
== [ DOCTEST/Schema Admins ]
name: DOCTEST/Schema Admins server-name: DSserv1
```

If you specify a Directory Service group name, the command returns information for only that group. For example:

```
name : DOCTEST/Developers
server-name : ADServ1
```

The `server-name` is the name you assigned to the Directory Service server when you configured it in the `user fsae` command.

vpn certificate

Display detailed information about local and CA certificates installed on the FortiGate. This is a VDOM level command. The global command is `get certificate`.

Syntax

```
get vpn certificate {local | ca} details [certificate_name]
```

vpn ike gateway

Use this command to display information about FortiGate IPsec VPN IKE gateways.

Syntax

```
get vpn ike gateway [<gateway_name_str>]
```

vpn ipsec tunnel details

Use this command to display detailed information about IPsec tunnels.

Syntax

```
get vpn ipsec tunnel details
```

vpn ipsec tunnel name

Use this command to display information about a specified IPsec VPN tunnel.

Syntax

```
get vpn ipsec tunnel name <tunnel_name_str>
```

vpn ipsec tunnel summary

Use this command to display summary information about IPsec tunnels.

Syntax

```
get vpn ipsec tunnel summary
```

vpn ipsec stats crypto

Use this command to display information about the FortiGate hardware and software crypto configuration.

Syntax

```
get vpn ipsec stats crypto
```

Example output

```
get vpn ipsec stats crypto
IPsec crypto devices in use:
```

```
CP6 (encrypted/decrypted):
  null:  0    0
  des:   0    0
  3des:  0    0
  aes:   0    0
CP6 (generated/validated):
  null:  0    0
  md5:   0    0
  sha1:  0    0
  sha256: 0    0

SOFTWARE (encrypted/decrypted):
  null:  0    0
  des:   0    0
  3des:  0    0
  aes:   0    0
SOFTWARE (generated/validated):
  null:  0    0
  md5:   0    0
  sha1:  0    0
  sha256: 0    0
```

vpn ipsec stats tunnel

Use this command to view information about IPsec tunnels.

Syntax

```
get vpn ipsec stats tunnel
```

Example output

```
#get vpn ipsec stats tunnel
tunnels
total: 0
static/ddns: 0
dynamic: 0
manual: 0
errors: 0
selectors
total: 0
up: 0
```

vpn ssl monitor

Use this command to display information about logged in SSL VPN users and current SSL VPN sessions.

Syntax

```
get vpn ssl monitor
```

Example output**vpn status l2tp**

Use this command to display information about L2TP tunnels.

Syntax

```
get vpn status l2tp
```

vpn status pptp

Use this command to display information about PPTP tunnels.

Syntax

```
get vpn status pptp
```

vpn status ssl

Use this command to display SSL VPN tunnels and to also verify that the FortiGate unit includes the CP6 or greater FortiASIC device that supports SSL acceleration.

Syntax

```
get vpn status ssl hw-acceleration-status
get vpn status ssl list
```

Variable	Description
hw-acceleration-status	Display whether or not the FortiGate unit contains a FortiASIC device that supports SSL acceleration.
list	Display information about all configured SSL VPN tunnels.

webfilter categories

List the FortiGuard Web Filtering categories.

Syntax

```
get webfilter categories
```

Example output (partial)

```
FG-5KD3914800284 # get webfilter categories
```

```
g01 Potentially Liabile:
  1 Drug Abuse
  3 Hacking
  4 Illegal or Unethical
  5 Discrimination
  6 Explicit Violence
 12 Extremist Groups
 59 Proxy Avoidance
 62 Plagiarism
 83 Child Abuse
g02 Adult/Mature Content:
  2 Alternative Beliefs
  7 Abortion
  8 Other Adult Materials
  9 Advocacy Organizations
 11 Gambling
 13 Nudity and Risque
 14 Pornography
 15 Dating
 16 Weapons (Sales)
 57 Marijuana
 63 Sex Education
 64 Alcohol
 65 Tobacco
 66 Lingerie and Swimsuit
 67 Sports Hunting and War Games
g04 Bandwidth Consuming:
 19 Freeware and Software Downloads
 24 File Sharing and Storage
 25 Streaming Media and Download
 72 Peer-to-peer File Sharing
 75 Internet Radio and TV
 76 Internet Telephony
g05 Security Risk:
 26 Malicious Websites
 61 Phishing
 86 Spam URLs
 88 Dynamic DNS
    ...
```

webfilter ftgd-statistics

Use this command to display FortiGuard Web Filtering rating cache and daemon statistics.

Syntax

```
get webfilter ftgd-statistics
```

Example output

```
get webfilter ftgd-statistics

Rating Statistics:
=====
DNS failures : 0
DNS lookups : 0
Data send failures : 0
Data read failures : 0
Wrong package type : 0
Hash table miss : 0
Unknown server : 0
Incorrect CRC : 0
Proxy request failures : 0
Request timeout : 0
Total requests : 0
Requests to FortiGuard servers : 0
Server errored responses : 0
Relayed rating : 0
Invalid profile : 0

Allowed : 0
Blocked : 0
Logged : 0
Errors : 0

Cache Statistics:
=====
Maximum memory : 0
Memory usage : 0

Nodes : 0
Leaves : 0
Prefix nodes : 0
Exact nodes : 0

Requests : 0
Misses : 0
Hits : 0
Prefix hits : 0
Exact hits : 0

No cache directives : 0
Add after prefix : 0
Invalid DB put : 0
DB updates : 0

Percent full : 0%
Branches : 0%
Leaves : 0%
Prefix nodes : 0%
```

```
Exact nodes : 0%

Miss rate : 0%
Hit rate : 0%
Prefix hits : 0%
Exact hits : 0%
```

webfilter status

Use this command to display FortiGate Web Filtering rating information.

Syntax

```
get webfilter status [<refresh-rate_int>]
```

wireless-controller client-info

Use this command to get information about WiFi clients.

Syntax

```
get wireless-controller client-info <vfid> <interface> <client_ip>
```

The output looks like this:

```
# get wireless-controller client-info 0 test-local 192.168.2.100
count=1
status: sta_mac=10:fe:ed:26:aa:e0 ap_sn=FP320C3X14006184, ap_name=FP320C3X14006184,
      chan=6, radio_type=11N
```

wireless-controller rf-analysis

Use this command to show information about RF conditions at the access point.

Syntax

```
get wireless-controller rf-analysis [<wtp_id>]
```

Example output

```
# get wireless-controller rf-analysis
<wtp-id> wtp id

FWF60C3G11004319 (global) # get wireless-controller rf-analysis
WTP: FWF60C-WIFI0 0-127.0.0.1:15246
channel rssi-total rf-score overlap-ap interfere-ap
1 418 1 24 26
2 109 5 0 34
3 85 7 1 34
4 64 9 0 35
```

```
5 101 6 1 35
6 307 1 8 11
7 82 7 0 16
8 69 8 1 15
9 42 10 0 15
10 53 10 0 14
11 182 1 5 6
12 43 10 0 6
13 20 10 0 5
14 8 10 0 5
Controller: FWF60C3G11004319-0
channel rssi_total
1 418
2 109
3 85
4 64
5 101
6 307
7 82
8 69
9 42
10 53
11 182
12 43
13 20
14 8
```

wireless-controller scan

Use this command to view the list of access points detected by wireless scanning.

Syntax

```
get wireless-controller scan
```

Example output

CMW	SSID	BSSID	CHAN	RATE	S:N	INT	CAPS	ACT	LIVE	AGE	WIRED
UNN		00:0e:8f:24:18:6d	64	54M	16:0	100	Es	N	62576	1668	?
UNN	ftiguest	00:15:55:23:d8:62	157	130M	6:0	100	EPs	N	98570	2554	?

wireless-controller spectral-info

Use this command to display wireless controller spectrum analysis.

Syntax

```
get wireless-controller spectral-info
```


wireless-controller status

Use this command to view the numbers of wtp sessions and clients.

Syntax

```
get wireless-controller status
```

Example output

```
# get wireless-controller status
Wireless Controller :
wtp-session-count: 1
client-count : 1/0
```

wireless-controller vap-status

Use this command to view information about your SSIDs.

Syntax

```
get wireless-controller vap-status
```

Example output

```
# get wireless-controller vap-status
WLAN: mesh.root
name : mesh.root
vdom : root
ssid : fortinet.mesh.root
status : up
mesh backhaul : yes
ip : 0.0.0.0
mac : 00:ff:0a:57:95:ca
station info : 0/0
WLAN: wifi
name : wifi
vdom : root
ssid : ft-mesh
status : up
mesh backhaul : yes
ip : 10.10.80.1
mac : 00:ff:45:e1:55:81
station info : 1/0
```

wireless-controller wlchanlistlic

Use this command to display a list of the channels allowed in your region, including the maximum permitted power for each channel

the channels permitted for each wireless type (802.11n, for example)

The list is in XML format.

Syntax

```
get wireless-controller wlchanlistlic
```

Sample output

```
country name: UNITED STATES2, country code:841, iso name:US
channels on 802.11A band without channel bonding:
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=165 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11B band without channel bonding:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11G band without channel bonding:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11N 2.4GHz band without channel bonding:
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

```
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 2.4GHz band with channel bonding plus:

```
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 2.4GHz band with channel bonding minus:

```
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 5GHz band without channel bonding:

```
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=165 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 5GHz band with channel bonding all:

```
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
```

wireless-controller wtp-status

Syntax

```
get wireless-controller wtp-status
```

Example output

```
# get wireless-controller wtp-status
```

```
WTP: FAP22B3U11005354 0-192.168.3.110:5246
wtp-id : FAP22B3U11005354
region-code :
name :
mesh-uplink : mesh
mesh-downlink : disabled
mesh-hop-count : 1
parent-wtp-id :
software-version :
local-ipv4-addr : 0.0.0.0
board-mac : 00:00:00:00:00:00
join-time : Mon Apr 2 10:23:32 2012
connection-state : Disconnected
image-download-progress: 0
last-failure : 0 -- N/A
last-failure-param:
last-failure-time: N/A
Radio 1 : Monitor
Radio 2 : Ap
country-name : NA
country-code : N/A
client-count : 0
base-bssid : 00:00:00:00:00:00
max-vaps : 7
oper-chan : 0
Radio 3 : Not Exist
WTP: FWF60C-WIFI0 0-127.0.0.1:15246
wtp-id : FWF60C-WIFI0
region-code : ALL
name :
mesh-uplink : ethernet
mesh-downlink : enabled
mesh-hop-count : 0
parent-wtp-id :
software-version : FWF60C-v5.0-build041
local-ipv4-addr : 127.0.0.1
board-mac : 00:09:0f:fe:cc:56
join-time : Mon Apr 2 10:23:35 2012
connection-state : Connected
image-download-progress: 0
last-failure : 0 -- N/A
last-failure-param:
last-failure-time: N/A
Radio 1 : Ap
country-name : US
country-code : N/A
client-count : 1
base-bssid : 00:0e:8e:3b:63:99
max-vaps : 7
oper-chan : 1
Radio 2 : Not Exist
Radio 3 : Not Exist
```

tree

The `tree` command displays FortiOS `config` CLI commands in a tree structure called the configuration tree. Each configuration command forms a branch of the tree.

Syntax

```
tree [branch] [sub-branch]
```

You can enter the `tree` command from the top of the configuration tree the command displays the complete configuration tree. Commands are displayed in the order that they are processed when the FortiGate unit starts up. For example, the following output shows the first 10 lines of `tree` command output:

```
tree
-- -- system -- [vdom] --*name (12)
+- vcluster-id (0,0)
|- <global> -- language
|- gui-ipv6
|- gui-voip-profile
|- gui-lines-per-page (20,1000)
|- admintimeout (0,0)
|- admin-concurrent
|- admin-lockout-threshold (0,0)
|- admin-lockout-duration (1,2147483647)
|- refresh (0,2147483647)
|- interval (0,0)
|- failtime (0,0)
|- daily-restart
|- restart-time
...

```

You can include a branch name with the `tree` command to view the commands in that branch:

```
tree user
-- user -- [radius] --*name (36)
    |- server (64)
    |- secret
    |- secondary-server (64)
    |- secondary-secret
    ...
|- [tacacs+] --*name (36)
    |- server (64)
    |- secondary-server (64)
    |- tertiary-server (64)
    ...
|- [ldap] --*name (36)
    |- server (64)
    |- secondary-server (64)
    |- tertiary-server (64)
    |- port (1,65535)
    ...

```

You can include a branch and sub branch name with the `tree` command to view the commands in that sub branch:

```
tree user local
-- [local] --*name (36)
|- status

```

```

|- type
|- passwd
|- ldap-server (36)
|- radius-server (36)
+- tacacs+-server (36)
...

```

If you enter the `tree` command from inside the configuration `tree` the command displays the tree for the current command:

```

config user ldap
tree
-- [ldap] --*name (36)
|- server (64)
|- cnid (21)
|- dn (512)
|- port (1,65535)
|- type
...

```

The `tree` command output includes information about field limits. These apply in both the CLI and the web-based manager. For a numeric field, the two numbers in parentheses show the lower and upper limits. For example (0,32) indicates that values from 0 to 32 inclusive are accepted. For string values, the number in parentheses is one more than the maximum number of characters permitted.

In the following example, the FQDN can contain up to 255 characters.

```

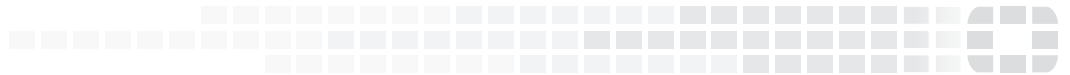
config firewall address
tree
-- [address] --*name (64)
|- subnet
|- type
|- start-ip
|- end-ip
|- fqdn (256)
|- country (3)
|- cache-ttl (0,86400)
|- wildcard
|- comment
|- visibility
|- associated-interface (36)
|- color (0,32)
+- [tags] --*name (64)

```



FORTINET®

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.